FORM PTO-1390 (REV. 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER 450101-02653
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	U.S. APPLICATION NO. (If known see 37 C.F.R. 1.5) 09/807703
INTERNATIONAL APPLICATION NO. PCT/JP00/05482 / INTERNATIONAL FILING DATE 16 AUGUST 2000	PRIORITY DATE CLAIMED 20 AUGUST 1999

TITLE OF INVENTION **INFORMATION RECORDING AND/OR REPRODUCING APPARATUS**

APPLICANT(S) FOR DO/EO/US **Tomoyuki ASANO, Yoshitomo OSAWA, Motoki KATO**

Applicants herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to promptly begin national examination procedures (35 U.S.C. 371(f)).
4. ☐ The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 – 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:

    PCT/RO/101, PCT/ISA/210
    PCT/IB/301, 304, 308
    16 Sheets of Drawings, 1 Page Abstract

EXPRESS MAIL

Mailing Label Number: **EL742695665US**

Date of Deposit: **April 17, 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents and Trademarks, Box PCT Washington, DC 20231.

Edward Ney
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.50)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NO.
09/807703	PCT/JP00/05482	450101-02653

21. ☒ The following fees are submitted

	CALCULATIONS PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5): Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO ..... $1000.00 International preliminary examination fee (37 C.F.R. 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... $860.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... $710.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4..... $690.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total Claims	92 - 20 =	72	x $18.00	$ 1,296.00
Independent Claims	14 - 3 =	11	x $80.00	$ 880.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $270.00	$

TOTAL OF ABOVE CALCULATIONS =	$
☐ Applicant claims small entity status. See 37 C.F.R. 1.27. The fees indicated above are reduced by ½. +	$
SUBTOTAL =	$
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).	$
TOTAL NATIONAL FEE =	$ 3,036.00
Fee for recording the enclosed assignments (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$ 40.00
TOTAL FEES ENCLOSED =	$ 3,076.00
Amount to be refunded:	$
Charged:	$

a. ☒ Two checks in the amount of **$ 3,076.00** to cover the above fees are enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **50-0320**. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. WARNING: Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

WILLIAM S. FROMMER, ESQ.
FROMMER LAWRENCE & HAUG LLP
745 FIFTH AVENUE
NEW YORK, NEW YORK 10151

Dated: April 17, 2001

William Frommer
SIGNATURE

WILLIAM S. FROMMER
NAME

25,506
REGISTRATION NUMBER

Description

Information Recording and/or Reproducing Apparatus

Technical Field

This invention relates to an information recording apparatus, an information reproducing apparatus, an information recording and reproducing apparatus, an information recording method, an information reproducing method, an information recording and reproducing method and a recording medium that enable to transmit and receive data safely.

Background Art

In recent years, recording apparatuses and recording media for recording information digitally are spreading. Since, for example, image and music data are recorded and reproduced with no deterioration in these recording apparatuses and recording media, the data can be copied repeatedly with the quality of the data maintained. From the viewpoint of copyright holders, however, there is a risk that the data the copyright of which they hold may be repeatedly and fraudulently copied with their quality maintained and distributed in the market. For this reason, it is necessary on the side of recording apparatuses and recording media to take appropriate measures to prevent copyrighted data from being fraudulently copied.

As a system for such copyright protection, in the minidisc (MD) (trademark)

system for example a method called SCMS (Serial Copy Management System) is used. This means information transmitted through a digital interface together with music data. This information shows under which of three types of data the music data contained fall: data for free copy, data copy once allowed or data copy prohibited. Upon receiving music data from the digital interface, a minidisc recorder detects an SCMS, and if it is copy prohibited, the music data are not recorded on the minidisc, and if it is copy once allowed, it is changed into copy prohibited and is recorded together with the music data received, and if it is copy free, it is recorded as it is together with the music data received.

In this way, in the minidisc system, the SCMS is used to prevent any fraudulent copy of copyrighted data.

Another method of preventing fraudulent copies of copyrighted data is a contents scramble system used in the Digital Versatile Disc (DVD) (trademark). In this system, all the copyrighted data on a disc are enciphered and only licenced recording apparatuses are given cipher keys which enable them to decipher and obtain meaningful data. And recording apparatuses are designed to ensure that all the operators observe the operation rules of not making fraudulent copies. In this way, the DVD system prevents copyrighted data from being fraudulently copied.

However, according to the system adopted by the minidisc system, there is a risk that recording apparatuses that do not follow the operating rule of changing the copy once allowed for theSCMS to the copy prohibited and recording the data received

may be manufactured illegally.

And although the system used by the DVD system is effective in ROM media, it is not effective in RAM media in which users can record data. This is because even in cases where unauthorized persons cannot decode the encryption, an illegal copy of the whole data on the disc into a new disc can produce a new disc that works on a licensed legitimate recording apparatus.

Therefore, in the Japanese Patent Application 10-25310 (Japanese Patent Application 1999-224461 Laid Open on August 17, 1999), information for identifying individual recording medium (hereinafter referred to as "medium identification information") are inscribed in it, and this information can only be accessed by licensed apparatuses. In other words, the data on each recording medium are enciphered by a medium identification information and a key based on a secret obtained by taking a license, and apparatuses that have not obtained license cannot decode the data that they may have read making such data meaningless. Furthermore, when a license is given to an apparatus, its operation is prescribed so that no fraudulent copy may be made. Unlicensed apparatuses cannot access medium identification information, and since medium identification information varies for each medium, even if a copy may be made by an unlicensed apparatus of all information accessible to it on a new medium, such new medium enables neither unlicensed apparatuses or licensed apparatuses to read information properly.

Meanwhile, the recording apparatus according to the Patent Application

includes for example an interface IEEE1394 capable of transmitting and receiving data to and from other apparatuses and may record contents data transmitted from other apparatuses on a recording medium.

In such a case, the contents data may be enciphered and transmitted by means of the Digital Transmission Content Protection Standard developed by Sony, Matsushita, Hitachi, Toshiba and Intel (this standard itself cannot be viewed without obtaining a license, but anybody can obtain a White Paper describing its outline from its licensing organization: Digital Transmission Licensing Administrator (DTLA)). The contents data are enciphered by means of a contents key Kc to be transmitted and the contents key Kc itself is enciphered. Such a safe method is used for transmission to the recording apparatuses. The simplest method for the recording apparatus to record on a recording medium the transmitted data safely, that is, without any fraudulent copy allowed is to record the contents data enciphered and transmitted as they are on the recording medium, and to encipher the contents key used for enciphering these data by means of the method used in this recording system and to record the same on the recording medium.

In this way, all that a recording apparatus must do at the time of recording is to simply receive and record a large volume of contents data, and the whole operation is simplified.

However, by the method described above, the contents data remain enciphered while they are transmitted to a recording apparatus and recorded on a medium, making

the reproduction operation inconvenient.

In other words, essentially at the time of reproducing AV contents, in order to perform trick plays (reproduction while performing a quick traverse or a quick return), the format and structure of the contents data must be identified and it is to be decided which data of the recording medium should be read in response thereto.

However, in the method described above, it is impossible to identify which data are recorded in which unit of the recording medium unless the contents data are read out from the recording medium and decoded, and therefore to finely control trick plays.

Disclosure of the invention

In view of such past problems, it is an object of the present invention to provide an information recording apparatus, an information reproducing apparatus, an information recording/reproducing apparatus, as well as an information recording method, an information reproducing method and an information recording/reproducing method capable of recording contents information on a recording medium and to finely control trick plays of this contents information.

It is another object of the present invention to provide a recording medium capable of finely controlling trick plays of the contents information recorded.

It is still another object of the present invention to provide an information recording apparatus, an information reproducing apparatus, and an information

recording/reproducing apparatus, as well as information recording method, an information reproducing method and an information recording/reproducing method capable of recording contents information enciphered and transmitted as they are on a recording medium, recording information for enciphering this contents information on a recording medium, and finely controlling trick plays.

It is still another object of the present information to provide a recording medium capable of recording enciphered contents information as it is and finely controlling trick plays of this contents information.

In order to achieve these objects, the information recording apparatus according to the present invention includes an inputting means for inputting contents information; a management information creating means for extracting the access positions for said contents information inputted and for creating management information showing one or more access positions for said contents information; and a writing means for writing said contents information inputted and said management information on a recording medium.

In one respect, the information reproducing apparatus according to the present invention includes a reading means for reading contents information and management information showing one or more access positions for said contents information from the recording medium containing said contents information and said management information; and a reading position controlling means for controlling the reading positions of said contents information on said recording medium based on said

management information read from said recording medium.

In another respect, the information recording/reproducing apparatus according to the present invention includes an inputting means for inputting contents information; a management information creating means for extracting access positions for said contents information inputted and for creating management information showing one or more access positions for said contents information; a reading means for reading said contents information and said management information from said recording medium; and a reading position controlling means for controlling the reading positions of said contents information on said recording medium.

In another respect, the information recording method according to the present invention includes the steps of inputting contents information; extracting access positions for said contents information inputted; creating management information showing one or more access positions for said contents information; and writing said contents information inputted and said management information on recording medium.

In another respect, the information reproducing method according to the present invention includes the steps of reading said contents information and said management information from a recording medium on which contents information and management information showing one or more access positions for said contents information; and controlling the reading positions of said contents information on said recording medium based on said management information read from said recording medium.

In another respect, the information recording/reproducing method according to

the present invention includes the steps of during the recording process, inputting contents information, extracting the access positions for said contents information inputted, creating management information showing one or more access positions for said contents information, and writing said contents information inputted on the recording medium; and during the reproducing process, reading said contents information and said management information from said recording medium, and controlling the reading positions of said contents information on said recording medium.

In another respect, the recording medium according to the present invention includes contents information, and management information extracted from said contents information and showing one or more access positions for this contents information being recorded.

In another respect, the information recording apparatus according to the present invention includes an inputting means for inputting enciphered contents information; a contents information decoding means for decoding said enciphered contents information; a management information creating means for extracting the access positions for said contents information from the contents information obtained by decoding enciphered contents information and for creating management information showing one or more access positions for said contents information; and a recording means for recording said enciphered contents information, information for enciphering said contents information as well as said management information created.

In another respect, the information reproducing apparatus according to the present invention includes a management information reading means for reading said contents information, information for enciphering said contents information and said management information from a recording medium in which enciphered contents information, information for enciphering said contents information and management information showing one or more access positions for said contents information; a reading position controlling means for controlling the reading positions of said enciphered contents information and information for enciphering said contents information; and a decoding means for decoding said enciphered contents information based on information for enciphering said contents information.

In another respect, the information recording/reproducing apparatus according to the present invention includes an inputting means for inputting enciphered contents information; a contents information decoding means for decoding said enciphered contents information; a management information creating means for creating management information showing one or more access positions for said contents information; a recording means for recording said enciphered contents information, information for enciphering said contents information, and said management information created on a recording medium; a management information reading means for reading enciphered contents information, information for enciphering said contents information and management information showing one or more access positions for said contents information from a recording medium on which said enciphered contents

information, information for enciphering said contents information and said management information are recorded; a reading position controlling means for controlling the reading positions for said enciphered contents information on said recording medium and information for enciphering said contents information based on the management information read from said recording medium; and a decoding means for decoding said enciphered contents information based on the information for enciphering said contents information.

In another respect, the information recording method according to the present invention includes the steps of inputting enciphered contents information; decoding said enciphered contents information; extracting the access positions for contents information from said contents information obtained by decoding enciphered contents information; creating management information showing one or more access positions for said contents information; and recording said enciphered contents information, information for enciphering said contents information and said management information created on the recording medium.

In another respect, the information reproducing method according to the present invention includes the steps of reading enciphered contents information, information for enciphering said contents information and management information showing one or more access positions for said contents information from a recording medium containing said enciphered contents information, information for enciphering said contents information and said management information; controlling the reading

positions for said enciphered contents information on said recording medium and information for enciphering said contents information; and decoding said enciphered contents information based on the information for enciphering said contents information.

In another respect, the information recording/reproducing method according to the present invention includes the steps of, during the recording process, inputting enciphered contents information, decoding said enciphered contents information, extracting the access positions for contents information from said contents information obtained by decoding enciphered contents information, creating management information showing one or more access positions for said contents information, and recording said enciphered contents information and information for enciphering said contents information as well as said management information created; and during the reproducing process, reading enciphered contents information, information for enciphering said contents information and management information showing one or more access positions for said contents information from a recording medium in which said enciphered contents information, information for enciphering said contents information and said management information are recorded; controlling the reading positions for said enciphered contents information and information for enciphering said contents information on said recording medium based on the management information read from said recording medium; and decoding said enciphered contents information based on information for enciphering said contents information.

In another respect, the recording medium according to the present invention serve to record enciphered contents information, information for enciphering said contents information, and management information extracted from said contents information and showing one or more access positions for said contents information.

Brief Description of Drawings

Fig. 1 is a block diagram showing the configuration of an optical disc recording/reproducing apparatus according to the present invention.

Fig. 2 is a drawing showing the overall configuration of data recorded in the optical disc.

Fig. 3 is a block diagram showing the specific configuration of the encryption processing unit in the optical disc recording/reproducing apparatus.

Fig 4 is a block diagram showing an example of the specific configuration of a map file creation circuit of the encryption processing unit.

Fig. 5 is a flow chart showing the operating process of a PAT/PMT analyzing unit of the map file creation circuit.

Fig. 6 is a conceptual rendering of a random access point list of video data in the MPEG system.

Fig. 7 is an explanatory schematic diagram of a transport stream and a map file.

Fig. 8 is a block diagram showing an example of specific configuration of a decoding processing unit of the optical disc storing/reproducing apparatus.

Fig. 9 is a block diagram showing an example of another configuration of the decoding processing unit.

Fig. 10 is a block diagram showing the configuration of a contents data reproducing apparatus for controlling the readout of contents data by means of information contained in the map file.

Fig. 11 is a flowchart showing the operating process of the encryption processing unit when user data are stored in an optical disc.

Fig. 12 is a flowchart showing the analysis process of the stream analysis unit of the map file creating circuit for analyzing video data transport packets.

Fig. 13 is a flowchart showing the analysis process of the stream analysis unit for analyzing audio data transport packets.

Fig. 14 is a flowchart showing the operating process of encryption processing unit when the user data is stored in an optical disc in which no media identification information DiscID is stored at the time of manufacturing.

Fig. 15 is a flowchart showing the reproducing process of user data in the decoding processing unit.

Fig. 16 is a flowchart showing the reproducing process of user data in the decoding processing unit.

Best Mode for Carrying out the Invention

The best mode for carrying out the invention is hereinafter explained with

reference to the drawings.

This invention is applied, for example, to an optical disc recording/reproducing apparatus 10 configured as shown in Fig. 1.

The optical disc recording/reproducing apparatus 10 shown in this Fig. 1 includes a spindle motor 12 for rotationally driving an optical disc 11, a recording/reproducing head 13 for optically scanning the information recording surface of the optical disc 11, a servo circuit 14 for controlling the spindle motor 12 based on reproduction signals obtained from the recording/reproducing head 13, a recording/reproducing unit 15 for recording/reproducing data through the optical disc 11 by means of the recording/reproducing head 13, and a control circuit 17 for controlling the servo circuit 14 and the recording/reproducing unit 15 based on setting information inputted from the input operating unit 16.

The spindle motor 12 rotationally drives the optical disc 11 at a constant linear velocity based on the control of the servo circuit 14.

The recording/reproducing head 13 optically scans the information recording surface of the optical disc 11 rotationally driven by the spindle motor 12 to record/ reproduce data.

The servo circuit 14 drives the spindle motor 12 so that the optical disc 11 may spin at a pre-set speed (for example at a constant linear velocity) and at the same time controls the tracking, focusing and threading of the recording/reproducing head 13.

The recording/reproducing unit 15 includes a nencryption processing unit 4 and

a decoding processing unit 5 operating under the control of the control circuit 17. The encryption processing unit 4 enciphers recording signals supplied from the outside, supplies enciphered recording signals to the recording/reproducing head 13 so that the same may be recorded on the optical disc 11. And the decoding processing unit 5 decodes the reproduced data that have been reproduced from the optical disc 11 by the recording/reproducing head 13 and outputs the same as reproduced signals to the outside.

The input operating unit 16 includes operation buttons not shown in figure, switches, remote controllers and so forth, and outputs signals corresponding to inputs operated by the user.

The control circuit 17 controls the whole apparatus according to a pre-set computer program stored in a memory not shown in figure.

In this mode of carrying out, the optical disc 11 includes, as shown in Fig. 2, a read-in-area AR read in and a data area AR data.

And in the read-in-area AR read in of the optical disc 11, E DiscID obtained by converting the identification information of the recording medium (hereinafter referred to for the sake of convenience as "DiscID") by a previously prescribed common method in the recording system (hereinafter referred to for the sake of convenience as "enciphered by a common security of the system") and an enciphered disc key EKd that has been obtained by enciphering a disc key Kd used for enciphering contents data given to each disc by an effective master key Kem created according to the medium

identification information DiscID allocated to the disc are recorded.

Incidentally, the method for converting medium identification information DiscID, i.e. the common security for the system is given by the copyright holder or a license manager approved by the copyright holder (for example, a licensor of recording media format) to licensees together with the master key Km described below at the time when a license is granted properly.

For example, one of the methods for converting medium identification information DiscID is to convert the medium identification information DiscID to information obtained by the time lag at the edge of bits representing the optical disc information by recording the same based on the pre-set M series codes. When such a conversion method is used, the recording of the medium identification information DiscID based on the pre-set M series codes and the M series codes become the common securities for the system. For this reason, it will be impossible to read (decode) the medium identification information DiscID unless both of them are known.

The encryption art based on such M series codes was already proposed by the present applicant in the Japanese Patent Application 9-288960 (corresponding U.S. Patent Application 09/174954: filed on October 9, 1998 to the U.S. Patent and Trademark Office). Incidentally, this pre-set common security for the system is given to the licensee together with the master key Km described below when a proper license is granted by the copyright holder.

The effective master key Kem is calculated according to the formula (1) by applying a hash function to the combination of the master key Km and the DiscID.

$$Kem = hash (Km + DiscID) \quad (1)$$

Here, the master key Km is a secret key given only to persons (optical disc recording/reproducing apparatus) properly licensed by the copyright holder. In addition, the combination of A and B, when each of them consists of 32 bits, means combining B after A to make 64-bit data.

And each sector Si (i = 1, 2, ...) constituting the data area AR data of the optical disc 11 consists of a header HD and a main data unit MD. The header HD stores a ciphered contents key EKc obtained by enciphering the contents key Kc used for enciphering contents data by the disc key Kd (the i of Si here means the number of the sector, but the i is omitted when it is unnecessary to distinguish individual sectors). The main data unit MD stores ciphered contents data obtained by enciphering contents data by the contents key Kc and received by the recording apparatus.

The encryption processing unit 4 in the optical disc recording/reproducing apparatus 10 of which the concrete configuration is shown in Fig. 3 includes a DiscID encryption decoding circuit 41, a Kem generating module 42, a random number generating circuit 43, a Kd encryption decoding circuit 44, a Kc encryption circuit 45, a contents data decoding circuit 46, and a map file creating circuit 47.

The DiscID encryption decoding circuit 41decodes E DiscID read from the read-in-area AR read in of the optical disc 11 by means of the recording/reproducing

head 13 based on the common security of the system kept in the DiscID encryption decoding circuit 41 and creates medium identification information DiscID. And this DiscID encryption decoding circuit 41 receives random numbers generated by the random number generating circuit 43 as medium identification information DiscID, enciphers the same based on the common security of the system as described above to create EDiscID. The EDiscID created from the random numbers by this DiscID encryption decoding circuit 41 are recorded in the read-in-area AR read in of the optical disc 11 through the recording/reproducing head 13.

The Kem generating module 42 includes a Km memory 42A for storing a master key Km and a hash function circuit 42B for creating effective master keys Kem based on the master key Km and medium identification information DiscID. The hash function circuit 42B generates the combination of the master key Km and a DiscID according to the formula (1), and applies the hash function to the same to create an effective master key Kem. And the hash function circuit 42B supplies the created effective master key Kem to the Kd encryption decoding circuit 44.

The Kd encryption decoding circuit 44 decodes by means of the effective master key Kem the enciphered disc key EKd read from the read-in-area AR read in of the optical disc 11 by the recording/reproducing 13 to create a disc key Kd. And this Kd enciphered decoding circuit 44 receives random numbers generated by the random number generating circuit 43 as a disc key Kd, enciphers the same by means of the effective master key Kem to create an enciphered disc key EKd. The enciphered disc

key EKd created by this Kd encryption decoding circuit 44 is stored in the read-in-area AR read in of the optical disc 11 through the recording/reproducing head 13.

The Kc encryption circuit 45 enciphers contents keys Kc that has been received from the interface with other apparatuses by means of the disc key Kd to create enciphered contents keys EKc. The enciphered contents keys EKc created by the Kc encryption circuit 45 are stored in the data area AR data of the optical disc 11 through the recording/reproducing head 13.

The enciphered contents data delivered by the interface unit are stored as they are in the data area AR data of the optical disc 11 through the recording /reproducing head 13.

The contents data decoding circuit 46 decodes contents data by means of the contents key Kc and supplies the same to the map file creating circuit 47.

The map file creating circuit 47 creates map files containing necessary information at the time of reproduction from the decoded contents data. The map files created by this map file creating circuit 47 are stored in the data area AR data of the optical disc 11 through the recording/reproducing head 13.

Here, the case in which contents data are MPEG2 transport stream will be explained with reference to the block diagram in Fig. 4 showing a specific example of configuration of the map file creating circuit 47.

This map file creating circuit 47 includes a PID filter 472 into which MPEG2 transport stream on which AV programs are multiplexed is inputted through a terminal

471, a PAT/PMT analysis unit 474 and a stream analysis unit 475 to which PID transport packets taken out of the PID filter 472 are supplied through a switch 473, a counter 476 to which PID transport packets taken out of the PID filter 472 are supplied, a map data creating unit 477 to which the results of analyses by the PAT/PMT analysis unit 474 and the stream analysis unit 475 are given, and a file system 478 connected to the map data creating unit 477.

The transport stream inputted through the terminal 471 is a stream made up of consecutive transport packets, and the transport packets are packeted MPEG2 video streams or MPEG1 audio streams.

The PID filter 472 takes out transport packets of specified PID from the inputted transport packets. The PID is a signal of 13-bit length located at the fixed position of the transport packet header, and shows the type of data stored in the payload (data portion following the transport packet header).

To begin with, the PID filter 472 takes out transport packets for a PAT (Program Association Table) of which PID = 0 x 0000. The PAT transport packets outputted from the PID filter 472 are inputted into the PAT/PMT analyzing unit 474 through a switch 473.

Here, the operating process of the PAT/PMT analyzing unit 474 will be explained by referring to a flowchart shown in Fig. 5.

At step S1, the PAT/PMT analyzing unit 474 receives PAT transport packets. PAT contains the PID of transport packets of the PMT (Program Map Table) of AV

programs multiplexed in the transport stream.

At step S2, the PAT/PMT analysis unit 474 sets the PID of the PMT of AV programs in the PID filter. After taking out transport packets carrying the PID of PMT, the PID filter 472 inputs them into the PAT/PMT analysis unit 474.

At step S3, the PAT/PMT analysis unit 474 receives transport packets of PMT. The PMT contains the PID of transport packets carrying a video stream or an audio stream constituting an AV program as their payloads. PAT/PMT analysis unit 474 acquires the PID of transport packets carrying video streams or audio streams constituting AV programs as their payloads.

At step S4, the PAT/PMT analysis unit 474 sets the PID of transport packets carrying a video stream or an audio stream constituting an AV program as their payloads in the PID filter and the stream analysis unit 475 to end the operating process.

And the PAT/PMT analysis unit 474 gives to the map data creating unit 477 the following parameters:

(A) The PID of transport packets of the PMT of an AV program,

(B) The PID of transport packets of video data constituting an AV program and the stream_type of the video data.

(C) The PID of transport packets of audio data constituting an AV program and the stream_type of the audio data.

(D) PCR_PID of the AV program.

Here, the steam_type means the contents of the PMT, and in the case of video data, it represents the stream-type of MPEG-2/MPEG-1 and in the case of audio data, it represents the stream-type of MPEG1/AC-3.

And the PID filter 472 takes out the video data transport packets and audio data transport packets specified by the PAT/PMT analysis unit 474 from the input transport stream, and inputs them into the stream analysis unit 475 through a switch 473. Transport packets other than the video data transport packets and audio data transport packets (such as service information packets) are not inputted into the stream analysis unit.

The transport packets outputted from the PID filter 472 are inputted into the counter 476. The counter 476 counts the number of bytes from the head packet of the transport stream to be recorded up to the current packet and gives the resulting value to the stream analysis unit 475.

The stream analysis unit 475 extracts points that can be accessed at random among the AV program for reproduction. The transport packets at the random access points of video data are packets having the sequence header of MPEG video data and the successive I picture data as their payloads. A conceptual rendering of the list of random access points is shown in Fig. 6. The random access points show the time stamp of transport packets to be accessed at random and the addresses for starting data readout. Here, the time stamp is calculated based on the input time to the recording apparatus of transport packets at the random access points or the PTS (Presentation

Time Stamp) of I pictures at the random access points. The PTS is information added to the header of PES packets according to the MPEG2 systems standard. Incidentally, this Fig. 6 shows transport stream files in a form of successive recording of transport packets. But a similar result can be achieved by adding time stamps showing the input time to the recording apparatus of the packet for each transport packet. This time stamp is similar to the 4-byte TSP_extra_header added to the transport packet prescribed by DV format for example.

The random access point information of video data and audio data is supplied to the map data creating unit 477. The map data creating unit 477 transforms the random access point information into tables.

The map data creating unit 477 gives the map data tables to the file system 478.

The file system 478 creates files out of the map data tables and outputs them.

Fig. 7 is an explanatory diagram of transport streams and map files. A map file contains the following data:

1. The PID of transport packets of the PMT of AV programs.

2. The PID of transport packets of video data constituting AV programs and the stream_type of video data.

3. The PID of transport packets of audio data constituting AV programs and the stream_type of audio data.

4. The PCR_PID of AV programs.

5. A list of random access points of AV video data.

6. A list of random access points of AV audio data.

The decoding processing unit 5 in the optical disc recording/reproducing apparatus 10, the specific configuration of which shown in Fig. 8, includes an EdiscId decoding circuit 51, a Kem generating module 52, a Kd decoding circuit 54 and a Kc decoding circuit 55.

The EDiscID decoding circuit 51 decodes EdiscID read by said recording/ reproducing head 13 from the read-in-area AR read in of the optical disc based on the common security of the system that it has and creates medium identification information DiscID. This EdiscID creating circuit 51 gives the created medium identification information to the Kem generating module 52.

The Kem generating module 52 includes a Km memory 52A that stores a master key Km and a hash function circuit 52 that creates an effective master key Kem from the master key Km and the medium identification information DiscID. The hash function circuit 52B creates the combination of the master key Km and DiscID according to the formula (1), and applies the hash function thereto to create an effective master key Kem. And the hash function circuit 41B supplies the created effective master key Kem to the Kd decoding circuit 54. This Kem generating module 52 is configured in the same way as the Kem generating module 42, and both may be used for double purposes.

The EKd decoding circuit 54 decodes an enciphered disc key EKd read by the recording/reproducing head 13 from the read-in-area AR read in of the optical disc 11

by means of the effective master key Kem to produce a disc key Kd.

The EKc decoding circuit 55 decodes the deciphered contents keys EKc stored in the header of various sectors Si read out by the recording/reproducing head 13 from the data area AR data of the optical disc 11by means of the disc key Kd to calculate a contents key Kc.

Meanwhile, the decoding processing unit 5 shown in Fig. 8 delivers contents data that have been read out while they remain ciphered and the decoded contents key Kc to the data interface. This is used for example when these contents are transmitted to other apparatuses.

On the other hand, the decoding processing unit 5 shown in Fig. 9 includes a contents decoding circuit 56 that decodes by means of a contents key Kc obtained by decoding by means of the EKc decoding circuit 55 the enciphered contents data read by the recording/reproducing head 13 from the data area AR data of the optical disc 11 to create clear text contents data.

The decoding processing unit 5 shown in this Fig. 9 is used for example in case where MPEG and other signals applied to these latter contents data in this reproducing apparatus are decoded and outputted as pictures through a D/A converter.

Incidentally, for starting this reproducing process, information contained in the map files created at the time of recording is used to control by means of the control circuit 17 the readout of contents data from the optical disc 11.

Fig. 10 is a block diagram showing the contents data reproducing apparatus for

controlling the readout of contents data by means of the information contained in map files. Here, a transport stream reproducing apparatus that uses information contained in the map files created in the map file creating circuit 47 described in Fig. 4 to control the readout of transport stream files corresponding to the map files will be explained.

A recording medium 60 contains transport stream files and their map files.

The reproduction control unit 65 instructs the read control unit 61 to read map files. The read control unit 61 reads map files from the recording medium 60. The map files are then processed at the decoding unit 62, the error correction unit 63 and the file system unit 64 to be inputted into the reproduction control unit 65.

The reproduction control unit 65 supplies the PID of PMT transport packets of AV programs, the PID of transport packets of video data constituting the programs, the stream_type of video data, the PID of transport packets of audio data constituting the programs, the stream_type of audio data and the PCR_PID to a demultiplexer and an AV decoder not shown.

When an instruction is given from the user interface to proceed to a random access reproduction, the reproduction control unit 65 determines the position of reading data from the recording medium 60 based on the contents of map data stored inside and inputs random access control information to the read control unit 61. When a program chosen by the user is to be reproduced from the middle at a certain time, for example, the reproduction control unit 65 finds out the nearest time stamp to the time specified from the list of time stamps, and instructs the read control unit 61 to read

data from an I picture located at the address of transport stream corresponding to the time stamp. And when a program chosen by the user is to be reproduced at a high speed, the reproduction control unit 65 instructs the read control unit 61 to read successively I pictures contained in the program based on data found at the random access point corresponding to the program.

The read control unit 61 reads data from the random access point designated, and the data read and processed by the decoding unit 62, the error correction unit 63 and the file system unit 64 are outputted as transport stream.

And now the processing procedure at the encryption processing unit 4 when user data are to be recorded in the optical disc 11 will be explained by referring to the flowchart shown in Fig. 11. In this case, however, we assume that the medium identification information DiscID is written in the optical disc 11 at the time of the manufacture of the optical disc 11.

To begin with, at step S11, the DiscID encryption decoding circuit 41receives an EDiscID or medium identification information DiscID that has been read from the read-in-area of the optical disc 11 and enciphered. At step S12, the DiscID encryption decoding circuit 41 further decodes the EdiscID based on the common security of the system that it has to create a DiscID and outputs the same to the hash function circuit 42B of the Kem generating module 42. The common security of the system was given by the copyright owner when a proper license was granted.

At step S13, the hash function circuit 42B of the Kem generating module 42

reads the master key Km from the Km memory 42A of the Kem generating module 42. And at step S14, the hash function circuit 42B of the Kem generating module 42 applies according to the formula (1) the hash function to the combination of medium identification information DiscID of the optical disc 11 and the master key Km to calculate an effective master key Kem and to supply the same to the Kd encryption decoding circuit 44.

Then at step S15, the Kd encryption decoding circuit 26 receives an enciphered disc key EKd read from the read-in-area of the optical disc 11. At step S16, the Kd encryption decoding circuit 26 determines whether an enciphered disc key EKd is written in the read-in-area of the optical disc 11 (whether it could receive an enciphered disc key EKd). When it is determined that no enciphered disc key EKd is written, the processing advances to step S17 and the random number generating circuit 43 generates a d-bit random number, specifically for example a 56-bit random number and outputs the same as a disc key Kd to the Kd encryption decoding circuit 44.

And at step S18, the Kd encryption decoding circuit 44 enciphers a disc key Kd supplied by the random number generating circuit 43 by means of an effective master key Kem that has been received from the hash function circuit 42B create an enciphered disc key EKd and stores the same in the read-in-area of the optical disc 11.

When it is determined at step S16 that an enciphered disc key EKd has been written, the processing advances to step S19, and the Kd encryption decoding circuit 44 decodes the enciphered disc key EKd that has been read from the read-in-area AR

read in of the optical disc 11 by means of an effective master key Kem that has been received from the hash function circuit 42B to create a disc key Kd. The Kd encryption decoding circuit 44 outputs the disc key Kd to the Kc encryption circuit 45.

After processing at step S18 or S19, at step S20, the Kc encryption circuit 45 receives a contents key Kc and enciphered contents data from the interface unit, and at step S21enciphers the contents key Kc by means of a disc key that has been received from the Kd encryption decoding circuit 44 (if an enciphered disc key EKd is recorded on the optical disc 11) or from the random number generating circuit 43 (if no enciphered disc key EKd is recorded on the optical disc 11) to create an enciphered contents key EKc. The Kc encryption circuit 45 also records the enciphered contents key EKc in the sector head that can be found in the data area of the optical disc 11.

Then at step S22, the contents data are recorded in the main data section of the data area of the optical disc 11.

At step S23, the contents data decoding circuit 46 decodes enciphered contents data by using a contents key Kc received from the interface to create clear text contents data, which will be delivered to the map file creating circuit 47.

At step S24, the map file creating circuit 47 (creates new map files if there is none and) extracts information required for reproduction from clear text contents data to add the same to the map files.

Examples of operation of the stream analysis unit 475 of the map file creating circuit 47 will be explained by referring to the flowcharts shown in Fig. 12 and Fig. 13.

Fig. 12 explains the analysis process of video data transport packets, while Fig. 13 explains the analysis process of audio data transport packets.

To begin with, the analysis process of video data transport packets will be explained by referring to a flowchart shown in Fig. 12.

At step S31, the PID of video data of AV programs to be recorded and their stream_type are inputted into the stream analysis unit 475 from the PAT/PMT analysis unit 404.

At step S32, the stream analysis unit 475 receives video data transport packets. The stream analysis unit 475 includes a video buffer. Upon receiving video data transport packets, the stream analysis unit 475 inputs the payload into the video stream buffer.

At step S33, the stream analysis unit 475 examines whether any stream contained in the video stream buffer contains any sequence_header_code of MPEG video data (32-bit signal of "0x000001B3"). Specifically, the question of whether there is anything matching with the sequence_header_code is examined by shifting by 1 byte from the stream head. Examined bytes is removed from the video stream buffer.

When at step S33 the stream contains no sequence_header_code, the processing returns to step S32. When step S32 is repeated twice or more, the video data packet payload is appended to the last data of the video buffer.

When at step S33 the stream contains any sequence_header_code, at step S34 transport packets containing the first byte of the sequence_header_code is made to be

the starting point for reading I picture data for making random accesses.

At step S35, the stream analysis unit 475 informs the starting point for reading the packet to the map data creating unit 477. The number of bytes counting from the head of the transport stream to be recorded as the address of random access point to the packet is inputted into the map data creating unit 477 by the counter unit 476, and the PTS (Presentation Time Stamp) of I pictures included in the packet payload is inputted as the time stamp of the random access point.

At step S36, the stream analysis unit 475 determines whether the current packet is the last input packet. If it is not the last packet, the processing returns to step S32. If it is the last packet, the processing ends.

And now the analyzing process of audio data transport packets will be explained by referring to Fig. 13.

At step S41, the PID of audio data of programs to be recorded and their stream_data are inputted by the PAT/PMT analysis unit 474 into the stream analysis unit 475.

At step S42, the stream analysis unit 475 receives audio data transport packets.

At step S43, the stream analysis unit 475 examines whether its payload of audio data stream contains any sinc_byte as the first byte of audio frames. Since the audio frame is of a fixed length determined by the codifying bit rate, the question of whether sync_bytes appearing at this fixed interval are included in this payload is examined.

If the payload does not include sync_bytes of audio frames at step S43, the

processing returns to step S42.

If the payload includes sync_bytes of audio frames at step S43, the processing advances to step S44.

At step S44, the stream analysis unit 475 informs the map data creating unit 477 that this is the starting point for reading audio frames in making random accesses to packets including sync_bytes of audio frames. The number of bytes counting from the head of the transport stream to be recorded as the address of random access point to the packet is inputted into the map data creating unit 477 by the counter unit 476, and the PTS (Presentation Time Stamp) of I pictures included in the packet payload is inputted as the time stamp of the random access point.

At step S45, the stream analysis unit 475 determines whether the current packet is the last input packet. If it is not the last packet, the processing returns to step S42. If it is the last packet, the processing ends.

And at step S25 of the flowchart shown in Fig. 11, various circuits of the encryption processing unit 4 determine whether all the contents data are recorded or not. When it is determined that all the contents data are not yet recorded, the processing advances to step S26, and various circuits of the encryption processing unit access sectors that have not recorded the data of the optical disc 11, returns to step S20 to repeat the same processing. If it is determined at step S45 that all the contents data have been recorded, various circuits of the encryption processing unit 4 ends all the recording operation.

By decoding in this way enciphered DiscID by means of the specified common security of the system given when a proper license was granted from the copyright owner and by obtaining thus medium identification information DiscID, enciphered information is recorded in the recording medium.

And now, the operational process in the encryption processing unit 4 by which user data are recorded on an optical disc 11 on which no medium identification information DiscID was recorded at the time of manufacture will be explained by referring to the flowchart shown in Fig. 14.

To begin with, at step S51, the DiscID encryption decoding circuit 21 receives an EdiscID read from the read-in-area AR read in of the optical disc 11, and the Kd encryption decoding circuit 44 receives an enciphered disc key EKd read from the read-in-area AR read in of the optical disc 11.

Then at step S52, the DiscID encryption decoding circuit 41 determines whether an EdiscID is written in the read-in-area AR read in of the optical disc 11 (whether it was possible to receive EdiscID or not), and the Kd encryption decoding circuit 44 determines whether an enciphered disc key EKd has been written in the read-in-area AR read in of the optical disc 11 (whether it has been possible to receive the enciphered disc key EKd). When it is determined that neither EdiscID nor enciphered disc key EKd has been written, the processing advances to step S53, and the random number generating circuit 43 generates I-bit, specifically 128-bit random numbers, and outputs them as medium identification information DiscID to the DiscID encryption

decoding circuit 41.

Then at step S54, the DiscID encryption decoding circuit 41 enciphers the medium identification information DiscID supplied by the random number generating circuit 43 by means of the common security of the system that it has, creates an EdiscID and records the same in the read-in-area AR read in of the optical disc 11.

Then at step S55, the hash function circuit 42B of the Kem generating module 42 reads the master key Km from the Km memory 42A of the Kem generating module 42. At step S56, according to the formula (1) above, the hash function circuit 42B of the Kem generating module 42 applies the hash function to the combination of the medium identification information DiscID of the optical disc 11 and the master key Km read from the Km memory 42A to create an effective master key Kem and supplies the same to the Kd encryption decoding circuit 44.

Then at step S57, the random generating circuit 43 generates d-bit or specifically 56-bit random numbers and output the same to the Kd encryption decoding circuit 44 as disc key Kd. At step S58, the Kd encryption decoding circuit 44 enciphers the disc key Kd received from the random generating circuit 43 by means of the effective master key Kem received from the hash function circuit 42B to create an enciphered disc key EKd and record the same in the read-in-area AR read in of the optical disc 11.

If it is determined at step S52 that the EdiscID and the enciphered disc key EKd are written, the processing advances to step S59, and the DiscID encryption decoding

circuit 41 decodes the EdiscID read from this optical disc 11 by means of the common security of the system that it has to create a medium identification information DiscID.

At step S60, the hash function circuit 42B of the Kem generating module 42 reads the master key Km from the Km memory 42A of the Kem generating module 42. The hash function circuit 42B of the Kem generating module 42 at step S61, according to the formula (1) above, applies the hash function to the combination of the DiscID of the optical disc 11 and the master key Km to calculate the effective master key Kem, and supplies the same to the Kd encryption decoding circuit 44.

Then at step S62, the Kd encryption decoding circuit 44 decodes an enciphered disc key EKd read from this optical disc 11 by means of an effective master key Kem received from the hash function circuit 42B to obtain a disc key Kd. The Kd encryption decoding circuit 44 outputs the disc key Kd to the Kc encryption circuit 45.

After the processing described at step S58 or step S62, the processing advances to step S63, and the processing performed at step S63 through step S70 are similar to the processing performed at steps S20 through S27 shown in Fig. 11, and when it is determined that all the contents data have been recorded, all the recording operations end.

The medium identification information DiscID is created and recorded in recording media as described above, and contents data enciphered in response to the medium identification information DiscID created and the master key Km are recorded on the recording medium. For this reason, those who have not been granted a proper

license from the copyright owner or license agents authorized by the copyright owner cannot reproduce contents data copied on existing recording media (recording media on which no DiscID is recorded) as meaningful information.

And now the reproducing process of user data performed by the decoding processing unit 5 will be explained by referring to the flowchart shown in Fig. 15. To begin with, at step S81, the EdiscID decoding circuit 51 receives enciphered medium identification information DiscID that has been read from the read-in-area AR read in of the optical disc 11 or EdiscID. Furthermore at step S82, the EdiscID decoding circuit 51 decodes the EdiscID based on the common security of the system that it has to create a medium identification information DiscID and outputs the same to the hash function circuit 52B of the Kem generating module 52.

Then at step S83, the hash function circuit 52B of the Kem generating module 52 receives a medium identification information DiscID outputted from the EdiscID decoding circuit 51, reads the master key Km from the Km memory 52A, applies the hash function to the combination of the medium identification information DiscID of the optical disc 11 and the master key Km according to the formula (1) to calculate an effective master key Kem, and supplies the same to the EKd decoding circuit 54.

At step S84, the EKd decoding circuit receives an enciphered disc key EKd read from the read-in-area AR read in of the optical disc 11. At step S85 the EKd decoding circuit 54 decodes this enciphered disc key EKd read by means of the effective master key Kem received from the hash function circuit 52B to calculate a disc key Kd and

outputs the same to the Ekc decoding circuit 55.

Then, at step S86, the control circuit 17 reads map files from the optical disc 11 and uses the same to determine the position for reading contents data.

At step S87, the EKc decoding circuit 55 receives the enciphered contents keys EKc of various sectors that have been read from the data area AR data of the optical disc 11. At step S88 the EKc decoding circuit 55 decodes the enciphered contents keys EKc that have been read by means of the disc key Kd received from the EKd decoding circuit 54 to calculate contents keys Kc and delivers them to the interface unit at step S89.

At step S90, the contents decoding circuit 56 reads enciphered contents data from the data area AR data of the optical disc 11 and delivers them to the interface unit.

Then at step S91, the question of whether various circuits of the decoding unit 5 have read all the necessary contents data from the data area AR data of the optical disc 11. When it is determined that all the contents data have not yet been read, the process operation advances to step S92 where various circuits of the decoding unit 5 are supplied with the data of the following sectors that have not yet been read of the optical disc 11 and repeats step S86 and the subsequent steps. When it is determined that all the necessary contents data are read, various circuits of the decoding unit 5 end the whole reproducing process.

The explanation above relates to, as shown in Fig. 8, process operations that

take place when contents data that have been read as they are enciphered and the decoded contents key Kc are to be delivered to the interface unit.

This is used in case where these contents are transmitted to other apparatuses.

On the other hand, an example of processing in the contents decoding circuit 56 in which enciphered contents data read by the recording/reproducing head 13 from the data area AR data of the optical disc 11 are decoded by means of a contents key Kc decoded by the EKc decoding circuit 55 to create clear contents data like the one in the decoding processing unit 5 shown in Fig. 9 will be explained by referring to the flowchart in Fig. 16.

This is used for example when MPEG and other signals applied to the latter contents are decoded in this reproducing apparatus to be outputted as pictures through a D/A converter.

Steps S101 through S108 in the flowchart shown in Fig. 16 are similar to the processing described at steps S81 through S88 in the flowchart shown in Fig. 15 and therefore their explanations will be omitted.

At step S109, the contents decoding circuit 56 decodes the enciphered contents data that have been read from the data area AR data of the optical disc 11 by means of a contents key Kc supplied by the EKc decoding circuit 55 to create clear text contents data and outputs the same for example to an MPEG decoder forming unit of this optical disc players.

At step S110, various circuits of the decoding unit 5determine whether all the

necessary contents data have been read from the data area AR data of the optical disc 11. When it is determined that all the contents data have not yet been read, the processing advances to step S111, where various circuits of the decoding unit 5 are supplied with data of the following sectors that have not been read of the optical disc 11 and repeats step S106 and the subsequent processing. When it is determined that all the necessary contents data have been read, various circuits of the decoding unit 5 end the whole reproduction processing.

By creating in this way the ID of recording media, enciphering them by means of the pre-set common security of the system and recording them on a recording medium, only those who are granted proper license from the copyright owner or a license manager authorized by the copyright owner are allowed to access the recording medium.

In the embodiment mentioned above, contents data and enciphered contents keys Ekc are recorded and reproduced by sector of an optical disc. However, this sector needs not always coincide with the physical sector of an optical disc and may be within previously fixed limits such as those formed by combining several physical sectors or logical sectors or limits set for each recording.

And in the mode of carrying out mentioned above, an enciphered contents key EKc is to be recorded in the header HD of each sector. However, instead of recording separately in each sector in this way, this may be bundled together and recorded in a lot for example in the read-in-area AR read in or the data area AR data. Incidentally,

when enciphered contents keys EKc are recorded separately in each sector, they can produce a stronger enciphering effect.

And in the mode of carrying out mentioned above, one disc key Kd is used for each optical disc. On this point, there is no need that it be limited to one. It is possible to use one such disc key in a previously fixed block of an optical disc and to use one for each recording.

And in the mode of carrying out mentioned above, map files may be enciphered by means of a contents key or a disc key and may be recorded on an optical disc.

And in the mode of carrying out mentioned above, enciphered contents keys EKc obtained by enciphering contents keys Kc are recorded on an optical disc. However, information for creating contents keys Kc may be enciphered by means of a disc key Kd and the result may be recorded on a disc. For example, by applying the hash function to contents key creating information for creating contents keys Kc, contents keys Kc may be obtained.

And this invention can be applied to the case in which data are recorded or reproduced on recording media other than optical discs.

Industrial Applicability

With the information recording apparatus, information reproducing apparatus, and information recording/reproducing apparatus as well as information recording method, information reproducing method and information recording/reproducing

method according to the present invention, it is possible to record contents information on the recording medium and to finely control trick plays of such contents information.

And with the recording medium according to the present invention, it is possible to finely control trick plays of contents information recorded.

And with the information recording apparatus, information reproducing apparatus and information recording/reproducing apparatus as well as the information recording method, information reproducing method and information recording/ reproducing method according to the present invention, it is possible to record contents information enciphered and transmitted as it is on the recording medium, to record on the recording medium information for enciphering contents information and still to finely control trick plays of such contents information.

And with the recording medium according to the present invention, enciphered contents information is recorded as it is and furthermore it is possible to finely control trick plays of contents information recorded.

Claims

1. An information recording apparatus comprising:

inputting means for inputting contents information;

management information creating means for extracting the access positions for said contents information inputted and for creating management information showing one or more access positions for said contents information; and

writing means for writing said contents information inputted and said management information on a recording medium.

2. The information recording apparatus according to claim 1 wherein said management information shows the access positions for the contents information by means of time information of such contents information and addresses on the recording medium.

3. The information recording apparatus according to claim 2 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems, and wherein

said management information shows the access positions for said contents information by means of the time stamps for said transport streams and addresses on the recording medium.

4. The information recording apparatus according to claim 1 wherein, as access positions described in the management information, positions where random accesses are possible to said contents information are extracted.

5. The information recording apparatus according to claim 4 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

6. An information reproducing apparatus comprising;

reading means for reading contents information and management information from a recording medium in which said contents information and said management information showing one or more access positions for said contents information are recorded; and

reading position controlling means for controlling the reading positions of said contents information on said recording medium based on said management information read from said recording medium.

7. The information reproducing apparatus according to claim 6 wherein said management information shows the access positions for the contents information by means of time information of the contents information and addresses on the recording medium.

8. The information reproducing apparatus according to claim 7 wherein said contents information is recorded on the recording medium in the form of transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents

information by means of the time stamps of said transport stream and addresses on the recording medium.

9. The information reproducing apparatus according to claim 6 wherein, as access positions described in said management information, positions where random accesses to said contents information are available are shown.

10. The information reproducing apparatus according to claim 9 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

as access positions described in said management information, transport packets each containing a sequence header code are shown.

11. An information recording/reproducing apparatus comprising:

inputting means for inputting contents information;

management information creating means for extracting access positions for said contents information inputted and for creating management information showing one or more access positions for said contents information;

recording means for recording said contents information inputted and said management information on a recording medium;

reading means for reading said contents information and said management information from said recording medium; and

reading position controlling means for controlling the reading positions of said contents information on said recording medium based on said management

information read from said recording medium.

12. The information recording/reproducing apparatus according to claim 11 wherein said management information shows the access positions for contents information by means of the time information of the contents information and addresses on the recording medium.

13. The information recording/reproducing apparatus according to claim 12 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and addresses on the recording medium.

14. The information recording/reproducing apparatus according to claim 11 wherein, as access positions described in said management information, positions where random accesses for said contents information are possible are extracted.

15. The information recording/reproducing apparatus according to claim 14 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

16. An information recording method comprising the steps of:

inputting contents information;

extracting access positions for said contents information inputted;

creating management information showing one or more access positions for said contents information; and

writing said contents information inputted and said management information on the recording medium.

17. The information recording method according to claim 16 wherein, said management information shows the access positions for contents information by means of the time information for the contents information and the addresses on the recording medium.

18. The information recording method according to claim 17 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps for said transport stream and the addresses on the recording medium.

19. The information recording method according to claim 16 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

20. The information recording method according to claim 19 wherein, said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are extracted.

21. An information reproducing method comprising the steps of:

reading contents information and management information from a recording medium on which said contents information and said management information showing one or more access positions for said contents information; and

controlling the reading positions of said contents information on said recording medium based on said management information read from said recording medium.

22. The information reproducing method according to claim 21 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

23. The information reproducing method according to claim 22 wherein, said contents information is recorded on a recording medium in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

24. The information reproducing method according to claim 21 wherein, as access positions described in said management information, positions where random accesses to said contents information are possible are shown.

25. The information reproducing method according to claim 24 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are indicated.

26. An information recording/reproducing method comprising the steps of:

during the recording process, inputting contents information, extracting the access positions for said contents information inputted, creating management information showing one or more access positions for said contents information, and writing said contents information inputted and said management information on the recording medium; and

during the reproducing process, reading said contents information and said management information from said recording medium, and controlling the reading positions of said contents information on said recording medium based on said management information read from said recording medium.

27. The information recording/reproducing method according to claim 26 wherein, said management information shows the access positions for contents information by means of the time information for the contents information and the addresses on the recording medium.

28. The information recording/reproducing method according to claim 27 wherein, said contents information is inputted in the form of transport streams prescribed by the

MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport stream and the addresses on the recording medium.

29. The information recording/reproducing method according to claim 26 wherein, as access positions described in said management information, positions where random accesses to said contents information are possible are extracted.

30. The information recording/reproducing method according to claim 29 wherein, said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are extracted.

31. A recording medium wherein,

contents information, and

management information extracted from said contents information and showing one or more access positions for this contents information are recorded.

32. An information recording apparatus comprising:

inputting means for inputting enciphered contents information;

contents information decoding means for decoding said enciphered contents information;

management information creating means for extracting the access positions for

said contents information from the contents information obtained by decoding enciphered contents information and for creating management information showing one or more access positions for said contents information; and

recording means for recording said enciphered contents information, information for enciphering said contents information as well as said created management information on a recording medium.

33. The information recording apparatus according to claim 32 further comprising:

receiving means for receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other apparatuses by means of communication means; and

cipher key enciphering means for creating enciphered cipher keys obtained by enciphering cipher keys received by said receiving means by the first cipher key, and wherein

said contents information decoding means uses the received cipher key to decode the enciphered contents information received to obtain contents information; and

said recording means records said enciphered cipher keys on said recording medium as information for enciphering said contents information.

34. The information recording apparatus according to claim 33 further comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher key by using recording medium identification information read from said

recording medium.

35. The information recording apparatus according to claim 33 further comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher key; and

second cipher key creating means for deciding the second cipher key used to encipher the first cipher key by using the recording medium identification information read from said recording medium.

36. The information recording apparatus according to claim 33 further comprising:

second cipher key creating means for deciding the second cipher key used to decode the first cipher key enciphered and read from said recording medium based on the recording medium identification information read from the said recording medium; and

the first cipher key decoding means for decoding the first cipher key enciphered by using said second cipher key created, wherein

said cipher key enciphering means enciphers the cipher keys received from said receiving means by using said first cipher key.

37. The information recording apparatus according to claim 32 further comprising:

receiving means for receiving enciphered contents information and the cipher keys used to encipher said contents information transmitted from other apparatuses by means of communication means;

cipher key creating information creating means for creating cipher key creating

information used to create cipher keys based on the cipher keys received from said receiving means; and

cipher key creating information creating means for creating enciphered cipher key creating information obtained by enciphering by the first cipher key said cipher key creating information created, and wherein

said contents information decoding means decodes the enciphered contents information received by means of cipher keys received to restore contents information; and wherein

said recording means records said enciphered cipher key creating information on said recording medium as information for enciphering said contents information.

38. The information recording apparatus according to claim 32 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

39. The information recording apparatus according to claim 38 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

40. The information recording apparatus according to claim 32 wherein, as access

positions described in said management information, positions where random accesses for said contents information are possible are extracted.

41. The information recording apparatus according to claim 40 wherein,

said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

42. An information reproducing apparatus comprising:

management information reading means for reading enciphered contents information, information for enciphering said contents information and management information from a recording medium in which said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded;

reading position controlling means for controlling the reading positions of said enciphered contents information on said recording medium and said information for enciphering said contents information; and

decoding means for decoding said enciphered contents information based on said information for enciphering said contents information.

43. The information recording apparatus according to claim 42 wherein, said recording medium contains an enciphered cipher key obtained by enciphering the

cipher key used for enciphering contents information as information for enciphering said contents information, and further comprising:

cipher key decoding means for decoding said enciphered cipher key by means of the first cipher key.

44. The information reproducing apparatus according to claim 43 further comprising:

first cipher key creating means for deciding the first cipher key used to decode said cipher key by said cipher key decoding means using the recording medium identification information read from said recording medium.

45. The information reproducing apparatus according to claim 43 further comprising:

first cipher key decoding means for decoding the first cipher key used to decode said cipher key using the second cipher key; and

second cipher key creating means for deciding the second cipher key used to decode said first cipher key by means of the recording medium identification information read from said recording medium.

46. The information reproducing apparatus according to claim 43 further comprising:

second cipher key creating means for deciding the second cipher key used to decode the first enciphered cipher key read from said recording medium based on the recording medium identification information read from said recording medium; and

first cipher key decoding means for decoding said first cipher key enciphered by means of said second cipher key created.

47. The information reproducing apparatus according to claim 42 wherein, said

recording medium contains enciphered cipher key creating information obtained by enciphering the cipher key creating information for creating the cipher keys used to encipher said contents information; and further comprising:

cipher key creating information decoding means for decoding said enciphered cipher key creating information by means of the first cipher key; and

cipher key creating means for creating said cipher key based on the cipher key creating information decoded by the first cipher key.

48. The information reproducing apparatus according to claim 42 wherein, said management information shows the access positions for contents information by means of the time information of the contents information and the addresses on the recording medium.

49. The information reproducing apparatus according to claim 48 wherein, said contents information is inputted by transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

50. The information reproducing apparatus according to claim 42 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

51. The information reproducing apparatus according to claim 50 wherein, said

contents information is inputted by transport streams prescribed by the MPEG 2 systems; and wherein

for access positions described in said management information, transport packets each containing a sequence header code are extracted.

52. An information recording/reproducing apparatus comprising:

inputting means for inputting enciphered contents information;

contents information decoding means for decoding said enciphered contents information;

management information creating means for extracting the access positions for contents information from said contents information decoded from said enciphered contents information and for creating management information showing one or more access positions for said contents information;

recording means for recording said enciphered contents information, information for enciphering said contents information, and said created management information on a recording medium;

management information reading means for reading enciphered contents information, said information for enciphering said contents information and said management information from said recording medium on which said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded;

a reading position controlling means for controlling the reading positions for said enciphered contents information on said recording medium and said information for enciphering said contents information based on the management information read from said recording medium; and

decoding means for decoding said enciphered contents information based on the information for enciphering said contents information.

53. The information recording/reproducing apparatus according to claim 52 further comprising:

receiving means for receiving enciphered contents information and the cipher keys used to encipher said contents information transmitted from other apparatuses by communication means;

cipher key enciphering means for creating enciphered cipher keys obtained by enciphering said cipher keys by means of the first cipher key; and

cipher key decoding means for decoding said enciphered cipher keys by means of the first cipher key, and wherein

said contents information decoding means decodes the enciphered contents information received by means of the cipher keys received to obtain contents information; and

said recording means records said enciphered cipher keys on said recording medium as information for enciphering said contents information.

54. The information recording/reproducing apparatus according to claim 53 further

comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher keys by means of the recording medium identification information read from said recording medium.

55. The information recording/reproducing apparatus according to claim 53 further comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher keys;

first cipher key decoding means for decoding the first cipher key used to decode said cipher keys by means of the second cipher key; and

second cipher key creating means for deciding the second cipher key used to encipher said first cipher key by means of the recording medium identification information read from said recording medium.

56. The information recording/reproducing apparatus according to claim 53 further comprising:

second cipher key creating means for deciding the second cipher key for decoding the first cipher key enciphered and read from said recording medium based on the recording medium identification information read from the said recording medium; and

first cipher key decoding means enciphered by means of the second cipher key created, and wherein

said cipher key enciphering means decodes the cipher keys received by said receiving means by means of said first cipher key.

57. The information recording/reproducing apparatus according to claim 52 further comprising:

receiving means for receiving enciphered contents information and the cipher keys used to encipher said contents information transmitted from other apparatuses by communication means;

cipher key creating information creating means for creating cipher key creating information used to create such cipher keys;

cipher key creating information enciphering means for creating enciphered cipher key creating information obtained by enciphering said cipher key creating information created by the first cipher key, and wherein

said contents information decoding means decodes the enciphered contents information received by means of the cipher key received to restore contents information; and

said recording means records said enciphered cipher key creating information on said recording medium as information for enciphering said contents information.

58. The information recording/reproducing apparatus according to claim 52 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

59. The information recording/reproducing apparatus according to claim 58 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

60. The information recording/reproducing apparatus according to claim 52 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

61. The information recording/reproducing apparatus according to claim 60 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

62. An information recording method comprising the steps of:

inputting enciphered contents information;

decoding said enciphered contents information;

extracting the access positions for contents information from said contents information obtained by decoding the enciphered contents information;

creating management information showing one or more access positions for said contents information; and

recording said enciphered contents information, information for enciphering said contents information and said created management information on a recording medium.

63. The information recording method according to claim 62 further comprising the steps of:

receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods using communication means;

creating enciphered cipher keys obtained by enciphering the received cipher keys by means of the first cipher key;

decoding the received enciphered contents information using the received cipher keys to restore contents information; and

recording said enciphered cipher keys on said recording medium as information for enciphering said contents information.

64. The information recording method according to claim 63 further comprising the step of:

deciding the first cipher key used to encipher said cipher keys using the recording medium identification information read from said recording medium.

65. The information recording method according to claim 63 further comprising the steps of:

deciding the first cipher key used to encipher said cipher keys; and

deciding the second cipher key used to encipher said first cipher key using the

recording medium identification information read by said recording medium.

66. The information recording method according to claim 63 further comprising the steps of:

deciding the second cipher key used to encipher the first cipher key enciphered and read from said recording medium based on the recording medium identification information read from said recording medium;

decoding the first cipher key enciphered by means of said created second cipher key; and

enciphering the received cipher keys using said first cipher key.

67. The information recording/reproducing method according to claim 62 further comprising the steps of:

receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods using communication means;

creating cipher key creating information for creating these cipher keys based on the received cipher keys;

creating enciphered cipher key creating information obtained by enciphering by the first cipher key said created cipher key creating information;

decoding the enciphered contents information received using the cipher keys received to restore contents information; and

recording said enciphered cipher key creating information on said recording medium as information for enciphering said contents information.

68. The information recording method according to claim 62 wherein, said management information shows the access positions for contents information by means of the time information for contents information and addresses on the recording medium.

69. The information recording method according to claim 68 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport packets and addresses on the recording medium.

70. The information recording method according to claim 62 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

71. The information recording method according to claim 70 wherein, said contents information is inputted in the form of transport packets prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

72. An information reproducing method comprising the steps of:

reading enciphered contents information, information for enciphering said contents information and management information from a recording medium in which

said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded;

controlling the reading positions for said enciphered contents information on said recording medium and said information for enciphering said contents information based on the management information read from said recording medium; and

decoding said enciphered contents information is decoded based on the information for enciphering said contents information.

73. The information reproducing method according to claim 72 wherein, said recording medium contains enciphered cipher keys obtained by enciphering cipher keys used to encipher contents information; and further comprising the step of:

decoding said enciphered cipher keys by the first cipher key.

74. The information reproducing method according to claim 73 further comprising the step of:

deciding the first cipher key used to decode said cipher keys by means of the recording medium identification information read from said recording medium.

75. The information reproducing method according to claim 73 further comprising the steps of:

decoding the first cipher key used to decode said cipher keys by means of the second cipher key; and

deciding the second cipher key used to decode said first cipher key by means

of the recording medium identification information read from said recording medium.

76. The information reproducing method according to claim 73 further comprising the steps of:

deciding the second cipher key for decoding the enciphered first cipher key read from said recording medium based on the recording medium identification information read from said recording medium; and

decoding said enciphered first cipher key by means of said created second cipher key.

77. The information reproducing method according to claim 72 wherein, said recording medium contains enciphered cipher key creating information obtained by enciphering cipher key creating information for creating cipher keys used to encipher said contents information; further comprising the steps of:

decoding said enciphered cipher key creating information by means of the first cipher key; and

creating said cipher keys based on the cipher key creating information decoded by means of the first cipher key.

78. The information reproducing method according to claim 72 wherein, said management information shows the access positions for contents information by means of the time information for contents information and addressed on the recording medium.

79. The information reproducing method according to claim 78 wherein, said contents

information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and addresses on the recording medium.

80. The information reproducing method according to claim 72 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

81. The information reproducing method according to claim 80 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

82. An information recording/reproducing method comprising the steps of:

during the recording process, inputting enciphered contents information, decoding said enciphered contents information, extracting the access positions for contents information from said contents information obtained by decoding enciphered contents information, creating management information showing one or more access positions for said contents information, and recording said enciphered contents information and information for enciphering said contents information as well as said created management information on a recording medium; and

during the reproducing process, reading said enciphered contents information, said information for enciphering said contents information and said management information from a recording medium in which said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded; controlling the reading positions for said enciphered contents information on said recording medium and information for enciphering said contents information based on the management information read from said recording medium; and decoding said enciphered contents information based on information for enciphering said contents information.

83. An information recording/reproducing method according to claim 82 further comprising the steps of:

during the recording process, receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods by communication means, creating enciphered cipher keys obtained by enciphering received cipher keys by means of the first cipher key, decoding the enciphered contents information received by means of the received cipher keys to restore contents information and recording said enciphered cipher keys are recorded on said recording medium as information for enciphering said contents information; and

during the reproducing process, decoding said enciphered cipher keys by means of the first cipher key.

84. An information recording/reproducing method according to claim 83 further comprising the step of:

deciding the first cipher key used to encipher said cipher keys by means of the recording medium identification information read from said recording medium.

85. An information recording/reproducing method according to claim 83 further comprising the steps of:

deciding the first cipher key used to encipher said cipher keys; and

deciding the second cipher key used to encipher said first cipher key by means of the recording medium identification information read from said recording medium.

86. An information recording/reproducing method according to claim 83 further comprising the steps of:

deciding the second cipher key for decoding the first enciphered cipher key read from said recording medium based on the recording medium identification information read from said recording medium; and

decoding the first enciphered cipher key by means of said second cipher key created; and wherein

the cipher keys received are decoded by means of said first cipher key.

87. An information recording/reproducing method according to claim 82 further comprising the steps of:

during the recording process, receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods

by communication means, creating cipher key creating information for creating these cipher keys based on the cipher keys received, creating enciphered cipher key creating information obtained by enciphering said created cipher key creating information by means of the first cipher key, decoding the received enciphered contents information received by means of the cipher keys received to restore contents information, and recording said enciphered cipher key creating information on said recording medium as information for enciphering said contents information; and

during the reproducing process, decoding said enciphered cipher key creating information by means of the first cipher key, and creating said cipher keys based on the cipher key creating information decoded by the first cipher key.

88. An information recording/reproducing method according to claim 82 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

89. An information recording/reproducing method according to claim 88 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

90. An information recording/reproducing method according to claim 82 wherein, as

access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

91. An information recording/reproducing method according to claim 90 wherein, said contents information is inputted in the form of transport packets prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

92. A recording medium wherein,

enciphered contents information,

information for enciphering said contents information, and

management information extracted from said contents information and showing one or more access positions for said contents information are recorded.

ABSTRACT

Contents data that have been enciphered and transmitted are recorded as they are on a recording medium, and the contents key used to encipher these data is enciphered in a way used in this recording system and is recorded on the medium. Moreover, a step is taken to ensure that fine trick plays can be performed. In recording contents data that have been enciphered and transmitted, the contents data themselves are recorded in the enciphered state on the recording medium. However, the contents data are decoded by a contents data decoding circuit 46, and a map file containing necessary management information for reproduction is created by a map file creating circuit 47 and this file is recorded together with the contents data.

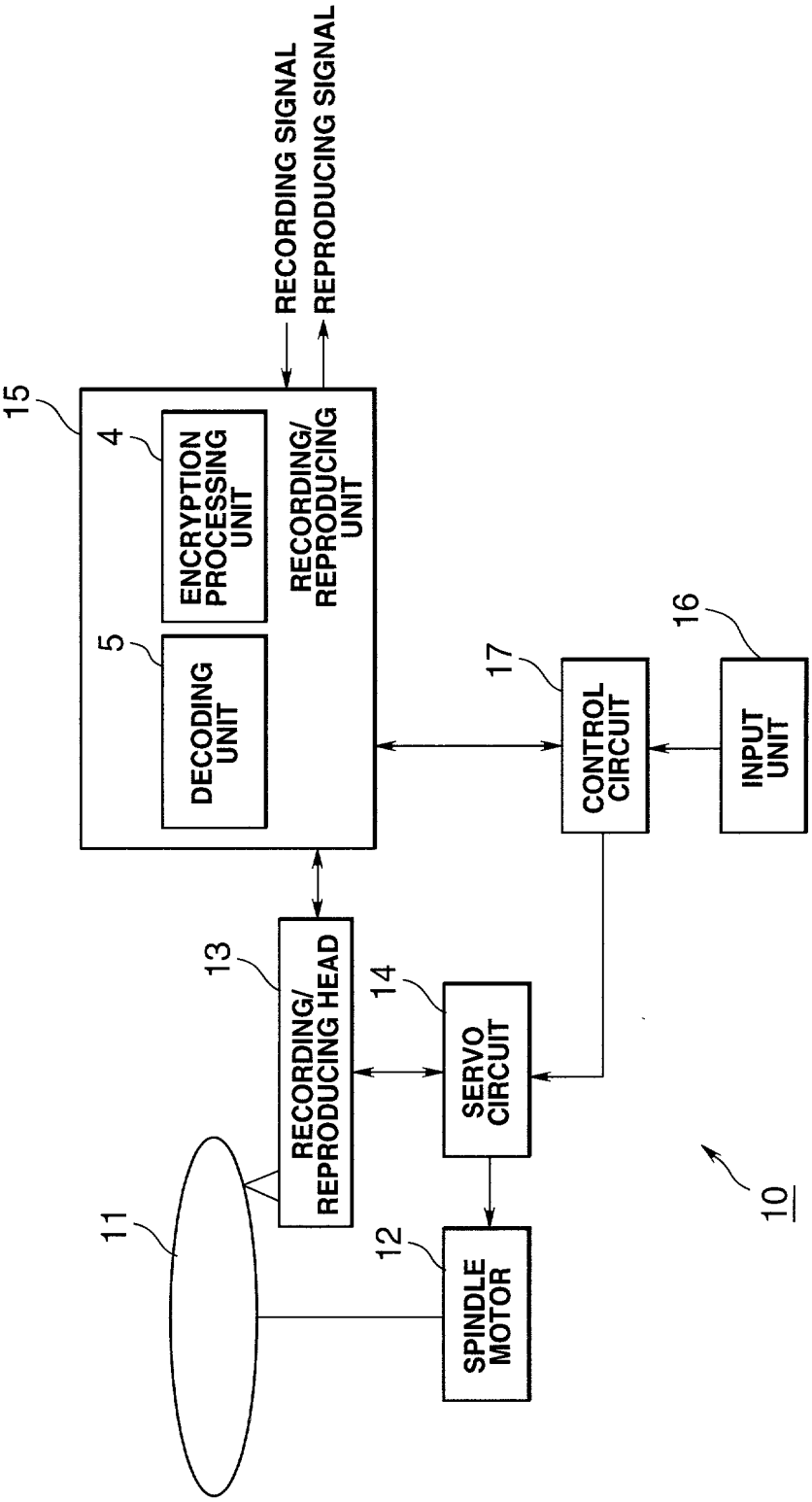

RECORDING SIGNAL
REPRODUCING SIGNAL
15
4
ENCRYPTION PROCESSING UNIT
5
DECODING UNIT
RECORDING/ REPRODUCING UNIT
17
CONTROL CIRCUIT
16
INPUT UNIT
13
RECORDING/ REPRODUCING HEAD
14
SERVO CIRCUIT
11
12
SPINDLE MOTOR
10

FIG.1

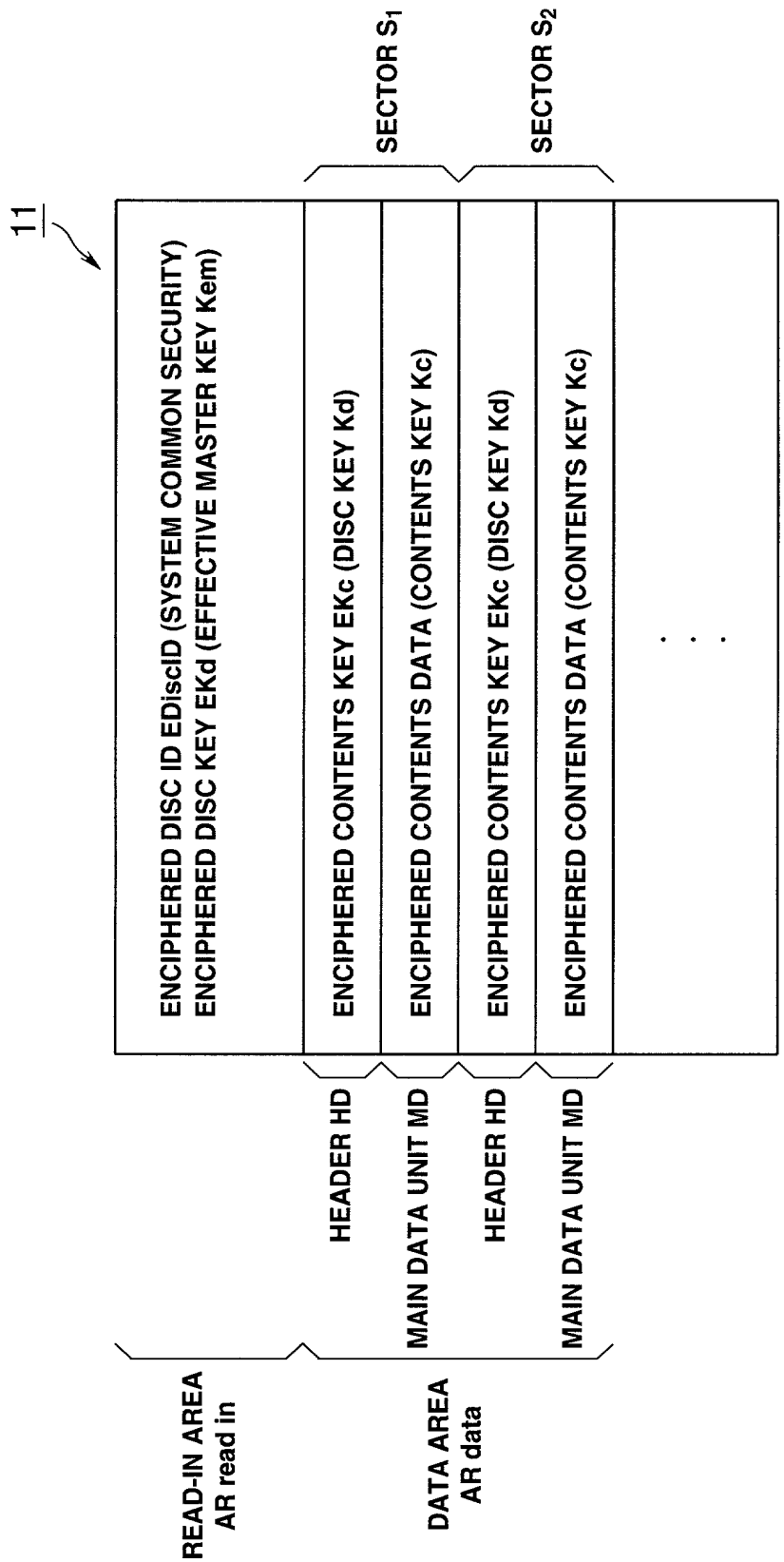

11
ENCIPHERED DISC ID EDisciD (SYSTEM COMMON SECURITY)
ENCIPHERED DISC KEY EKd (EFFECTIVE MASTER KEY Kem)
ENCIPHERED CONTENTS KEY EKc (DISC KEY Kd)
ENCIPHERED CONTENTS DATA (CONTENTS KEY Kc)
ENCIPHERED CONTENTS KEY EKc (DISC KEY Kd)
ENCIPHERED CONTENTS DATA (CONTENTS KEY Kc)
SECTOR S1
SECTOR S2
READ-IN AREA
AR read in
DATA AREA
AR data
HEADER HD
MAIN DATA UNIT MD
HEADER HD
MAIN DATA UNIT MD

FIG.2

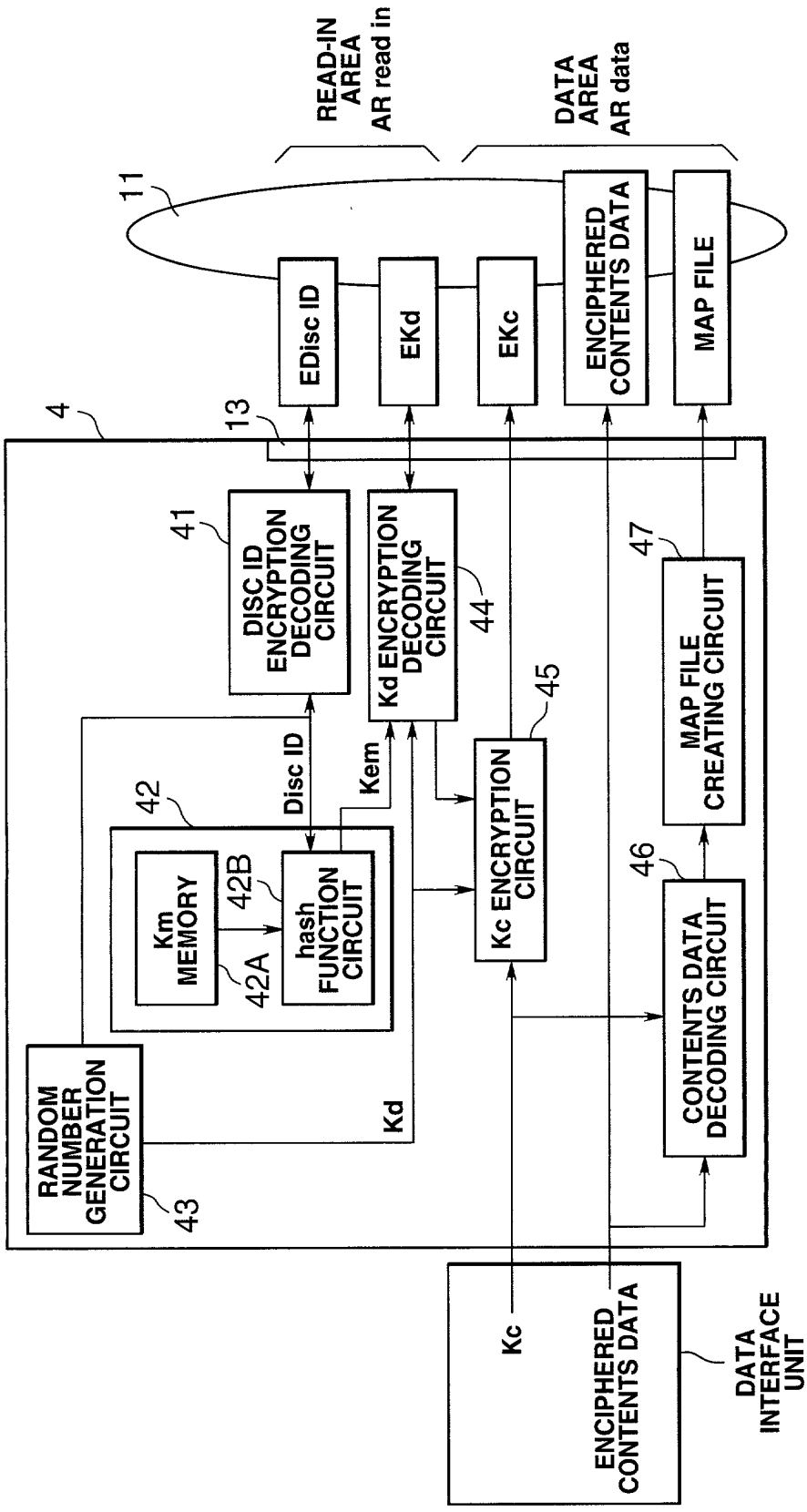

READ-IN AREA
AR read in
DATA AREA
AR data
11
EDisc ID
EKd
EKc
ENCIPHERED CONTENTS DATA
MAP FILE
4
13
41
DISC ID ENCRYPTION DECODING CIRCUIT
Kd ENCRYPTION DECODING CIRCUIT
44
47
MAP FILE CREATING CIRCUIT
45
Kc ENCRYPTION CIRCUIT
42
Km MEMORY
42B
hash FUNCTION CIRCUIT
42A
Disc ID
Kem
Kd
46
CONTENTS DATA DECODING CIRCUIT
RANDOM NUMBER GENERATION CIRCUIT
43
Kc
ENCIPHERED CONTENTS DATA
DATA INTERFACE UNIT

FIG.3

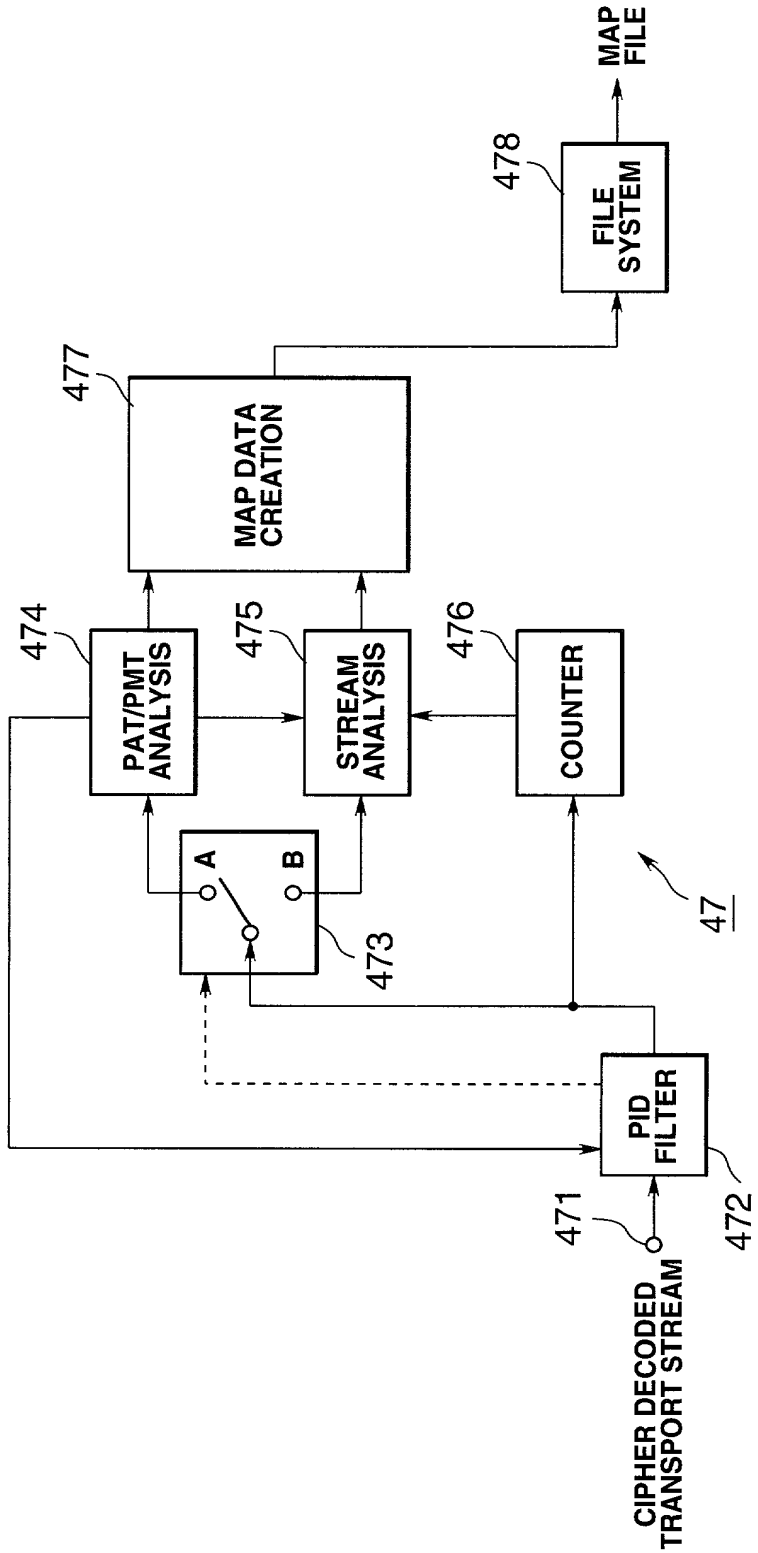

MAP FILE
478
FILE SYSTEM
477
MAP DATA CREATION
474
PAT/PMT ANALYSIS
475
STREAM ANALYSIS
476
COUNTER
A
B
473
47
PID FILTER
471
472
CIPHER DECODED TRANSPORT STREAM

FIG.4

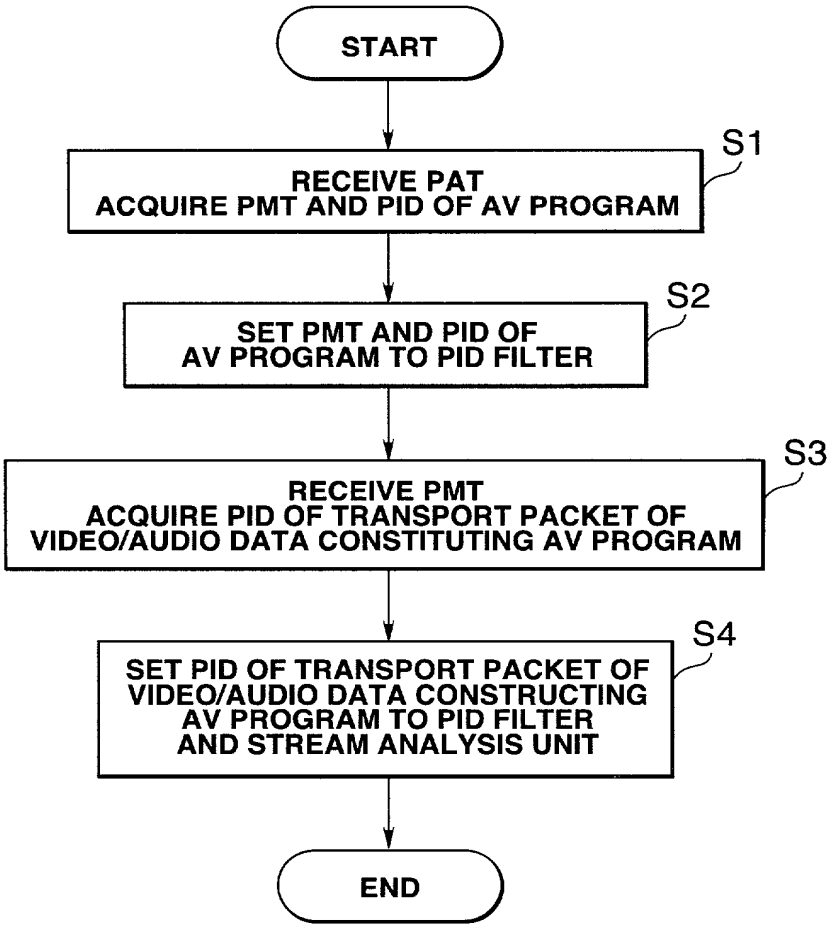
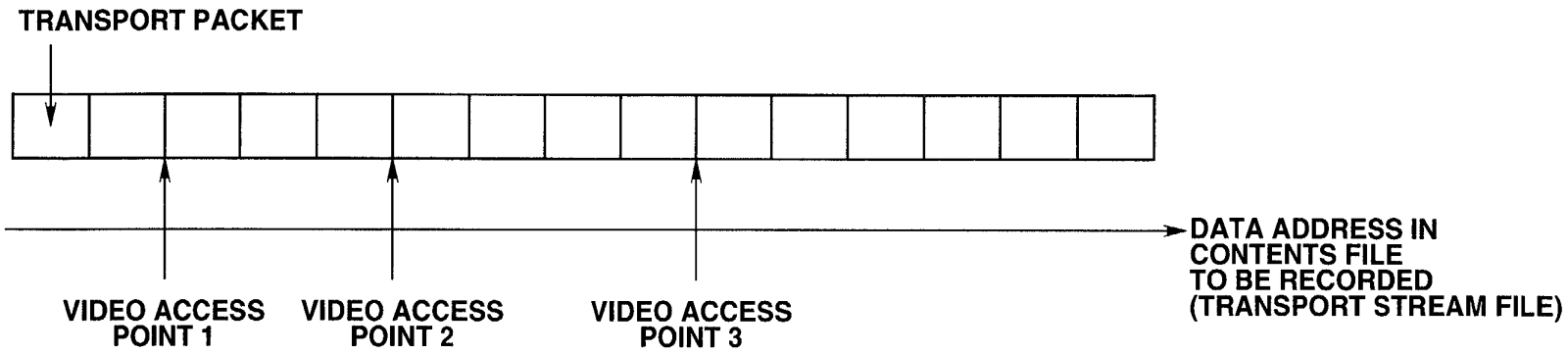

START
RECEIVE PAT
ACQUIRE PMT AND PID OF AV PROGRAM
S1
SET PMT AND PID OF
AV PROGRAM TO PID FILTER
S2
RECEIVE PMT
ACQUIRE PID OF TRANSPORT PACKET OF
VIDEO/AUDIO DATA CONSTITUTING AV PROGRAM
S3
SET PID OF TRANSPORT PACKET OF
VIDEO/AUDIO DATA CONSTRUCTING
AV PROGRAM TO PID FILTER
AND STREAM ANALYSIS UNIT
S4
END

FIG.5



LIST OF RANDOM ACCESS POINT OF VIDEO DATA

PID OF VIDEO PACKET
• TIME STAMP AND ADDRESS OF VIDEO ACCESS POINT 1 • TIME STAMP AND ADDRESS OF VIDEO ACCESS POINT 2 • TIME STAMP AND ADDRESS OF VIDEO ACCESS POINT 3 • • •

FIG.6

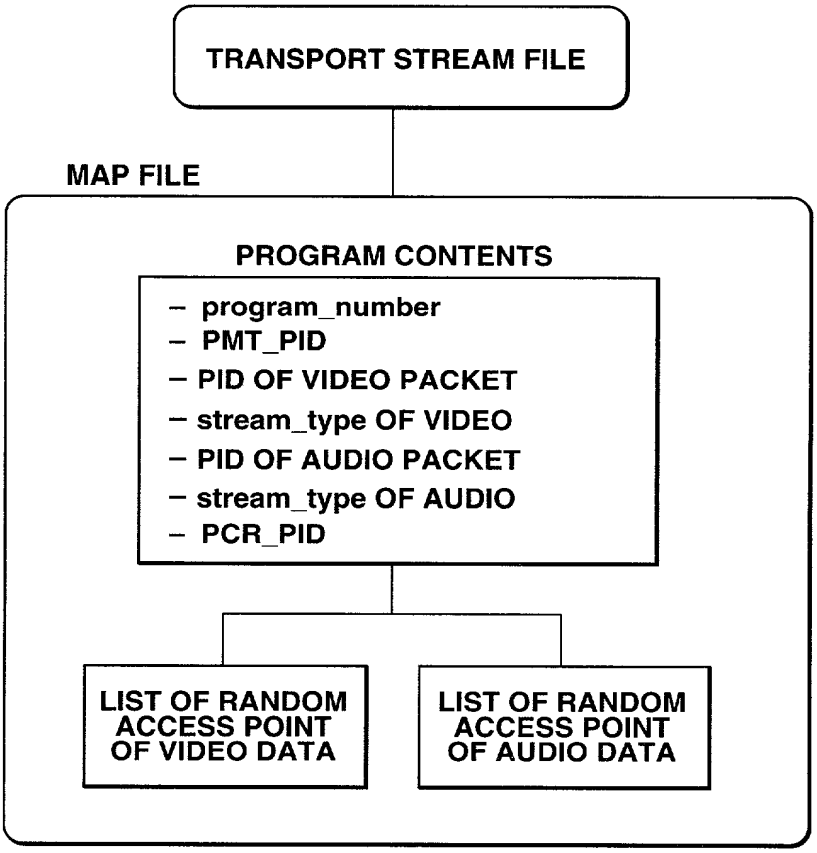

TRANSPORT STREAM FILE
MAP FILE
PROGRAM CONTENTS
– program_number
– PMT_PID
– PID OF VIDEO PACKET
– stream_type OF VIDEO
– PID OF AUDIO PACKET
– stream_type OF AUDIO
– PCR_PID
LIST OF RANDOM ACCESS POINT OF VIDEO DATA
LIST OF RANDOM ACCESS POINT OF AUDIO DATA

FIG.7

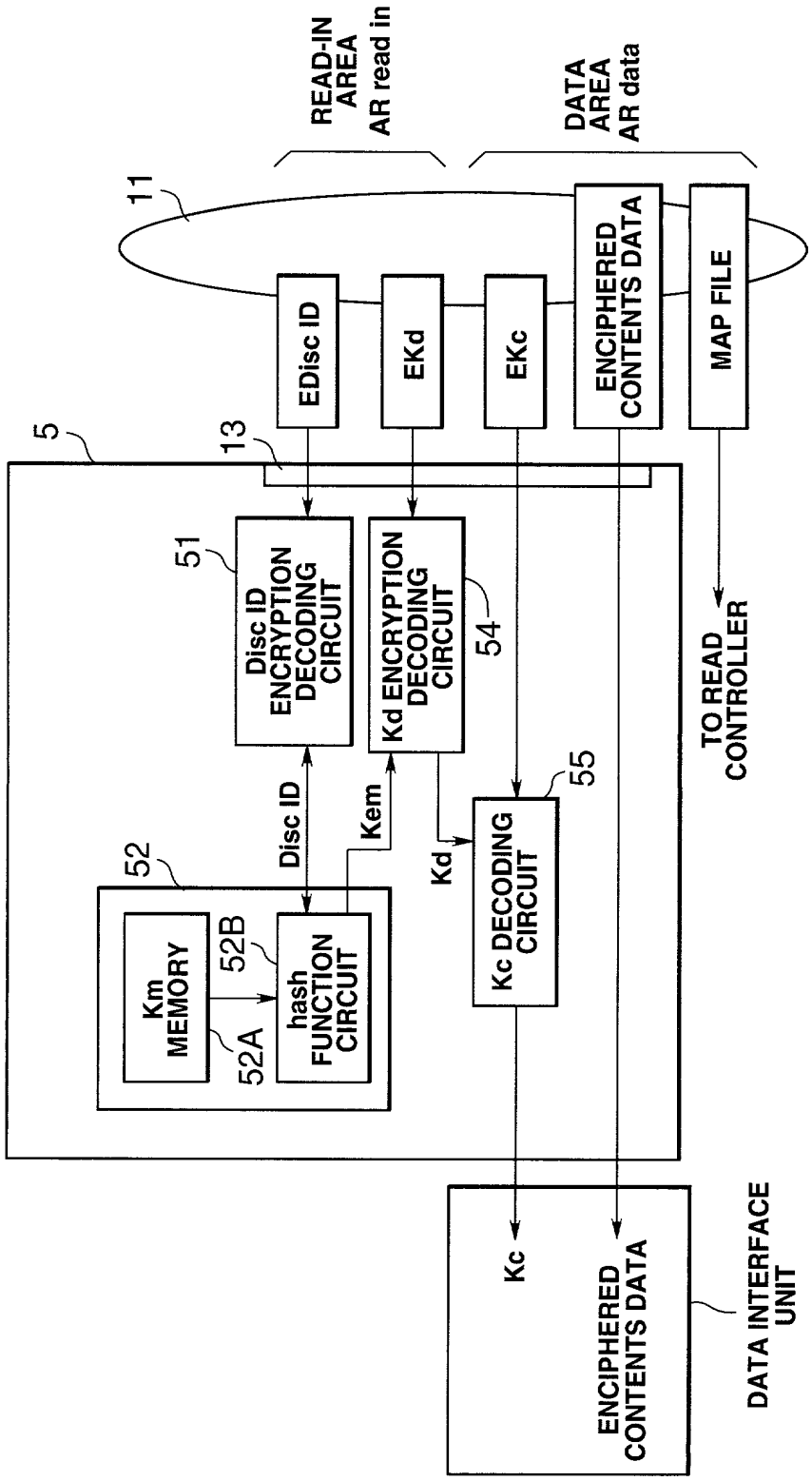

READ-IN AREA
AR read in
DATA AREA
AR data
11
EDisc ID
EKd
EKc
ENCIPHERED CONTENTS DATA
MAP FILE
5
13
51
Disc ID ENCRYPTION DECODING CIRCUIT
Kd ENCRYPTION DECODING CIRCUIT
54
TO READ CONTROLLER
Disc ID
Kem
Kd
55
Kc DECODING CIRCUIT
52
Km MEMORY
52B
hash FUNCTION CIRCUIT
52A
Kc
ENCIPHERED CONTENTS DATA
DATA INTERFACE UNIT

FIG.8

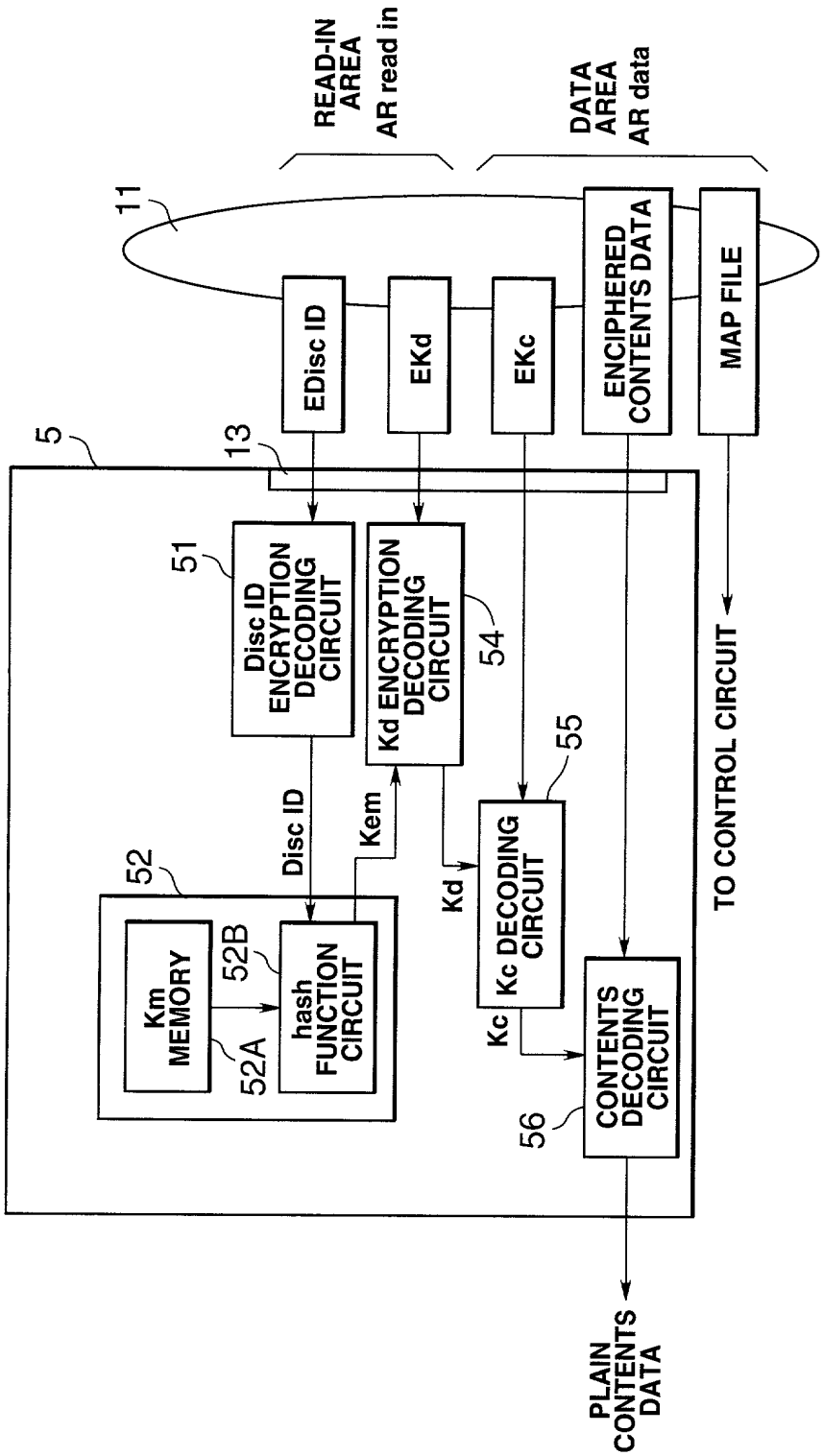

READ-IN AREA
AR read in
DATA AREA
AR data
11
EDisc ID
EKd
EKc
ENCIPHERED CONTENTS DATA
MAP FILE
5
13
51
Disc ID ENCRYPTION DECODING CIRCUIT
Kd ENCRYPTION DECODING CIRCUIT
54
55
Kc DECODING CIRCUIT
52
Km MEMORY
52A
52B
hash FUNCTION CIRCUIT
Disc ID
Kem
Kd
Kc
CONTENTS DECODING CIRCUIT
56
TO CONTROL CIRCUIT
PLAIN CONTENTS DATA

FIG.9

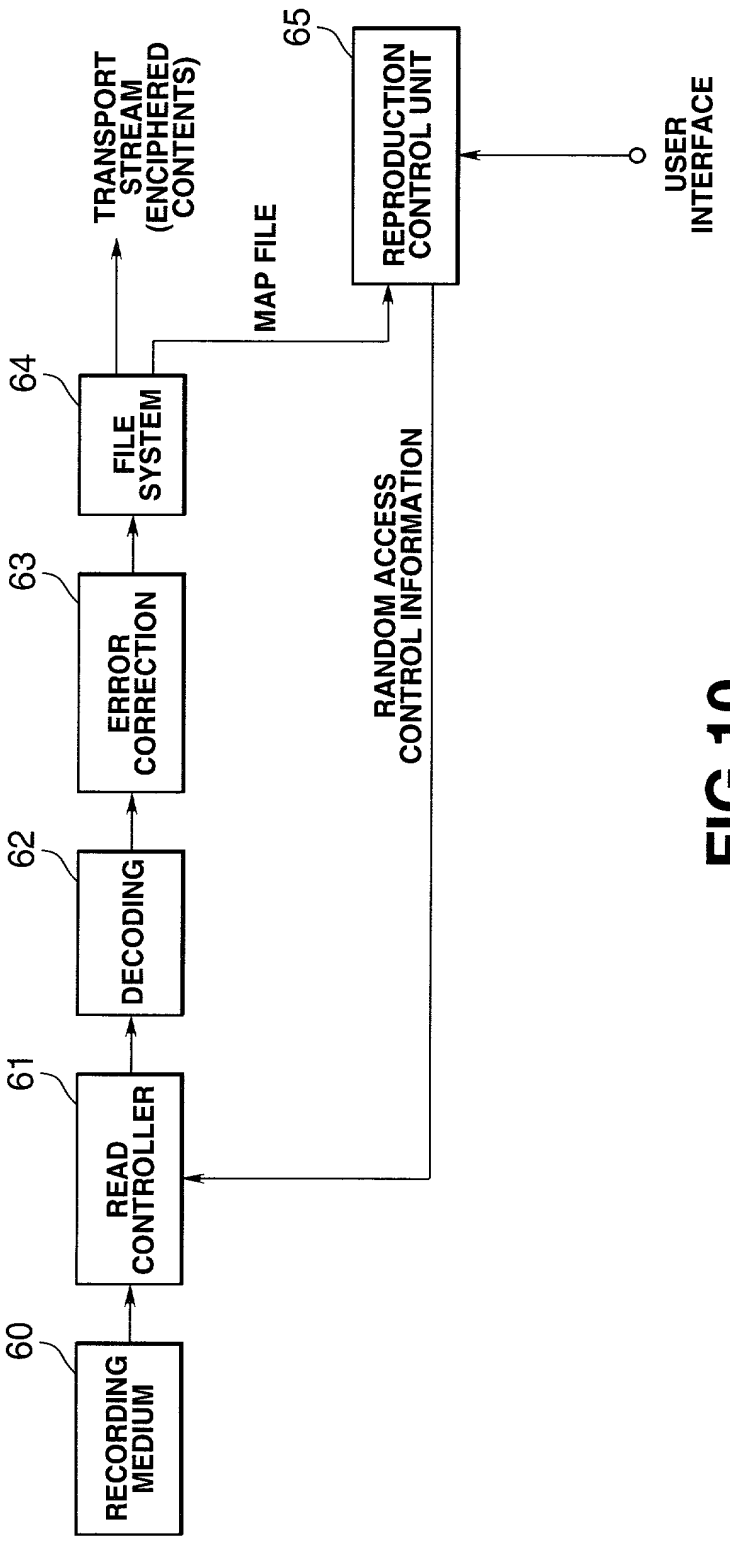

60
RECORDING MEDIUM
61
READ CONTROLLER
62
DECODING
63
ERROR CORRECTION
64
FILE SYSTEM
65
REPRODUCTION CONTROL UNIT
TRANSPORT STREAM (ENCIPHERED CONTENTS)
MAP FILE
RANDOM ACCESS CONTROL INFORMATION
USER INTERFACE

FIG.10

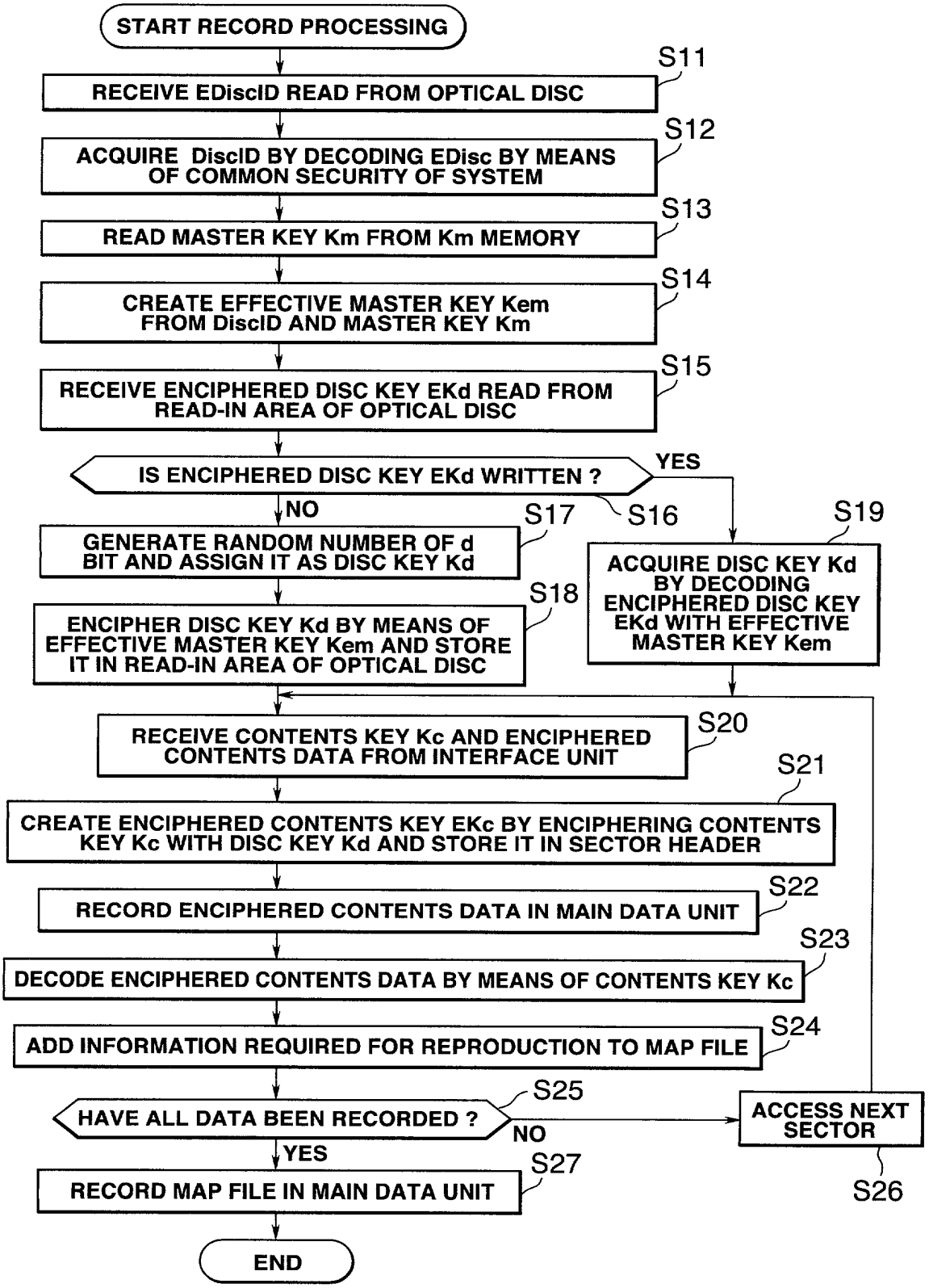

START RECORD PROCESSING
S11
RECEIVE EDiscID READ FROM OPTICAL DISC
S12
ACQUIRE DiscID BY DECODING EDisc BY MEANS OF COMMON SECURITY OF SYSTEM
S13
READ MASTER KEY Km FROM Km MEMORY
S14
CREATE EFFECTIVE MASTER KEY Kem FROM DiscID AND MASTER KEY Km
S15
RECEIVE ENCIPHERED DISC KEY EKd READ FROM READ-IN AREA OF OPTICAL DISC
IS ENCIPHERED DISC KEY EKd WRITTEN ?
YES
S16
NO
S17
GENERATE RANDOM NUMBER OF d BIT AND ASSIGN IT AS DISC KEY Kd
S18
ENCIPHER DISC KEY Kd BY MEANS OF EFFECTIVE MASTER KEY Kem AND STORE IT IN READ-IN AREA OF OPTICAL DISC
S19
ACQUIRE DISC KEY Kd BY DECODING ENCIPHERED DISC KEY EKd WITH EFFECTIVE MASTER KEY Kem
S20
RECEIVE CONTENTS KEY Kc AND ENCIPHERED CONTENTS DATA FROM INTERFACE UNIT
S21
CREATE ENCIPHERED CONTENTS KEY EKc BY ENCIPHERING CONTENTS KEY Kc WITH DISC KEY Kd AND STORE IT IN SECTOR HEADER
S22
RECORD ENCIPHERED CONTENTS DATA IN MAIN DATA UNIT
S23
DECODE ENCIPHERED CONTENTS DATA BY MEANS OF CONTENTS KEY Kc
S24
ADD INFORMATION REQUIRED FOR REPRODUCTION TO MAP FILE
S25
HAVE ALL DATA BEEN RECORDED ?
NO
YES
ACCESS NEXT SECTOR
S26
S27
RECORD MAP FILE IN MAIN DATA UNIT
END

FIG.11

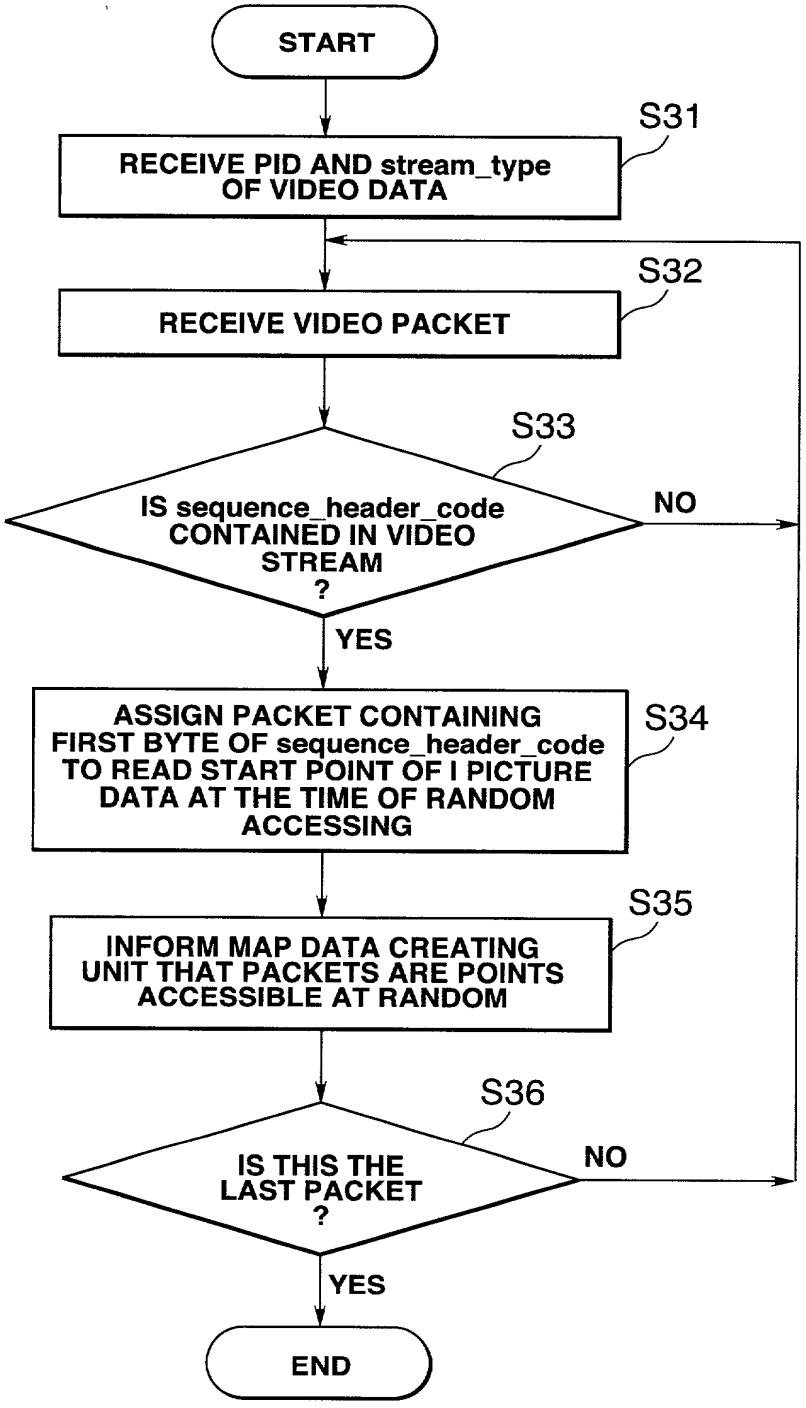

START
S31
RECEIVE PID AND stream_type OF VIDEO DATA
S32
RECEIVE VIDEO PACKET
S33
IS sequence_header_code CONTAINED IN VIDEO STREAM ?
NO
YES
ASSIGN PACKET CONTAINING FIRST BYTE OF sequence_header_code TO READ START POINT OF I PICTURE DATA AT THE TIME OF RANDOM ACCESSING
S34
INFORM MAP DATA CREATING UNIT THAT PACKETS ARE POINTS ACCESSIBLE AT RANDOM
S35
S36
IS THIS THE LAST PACKET ?
NO
YES
END

FIG.12

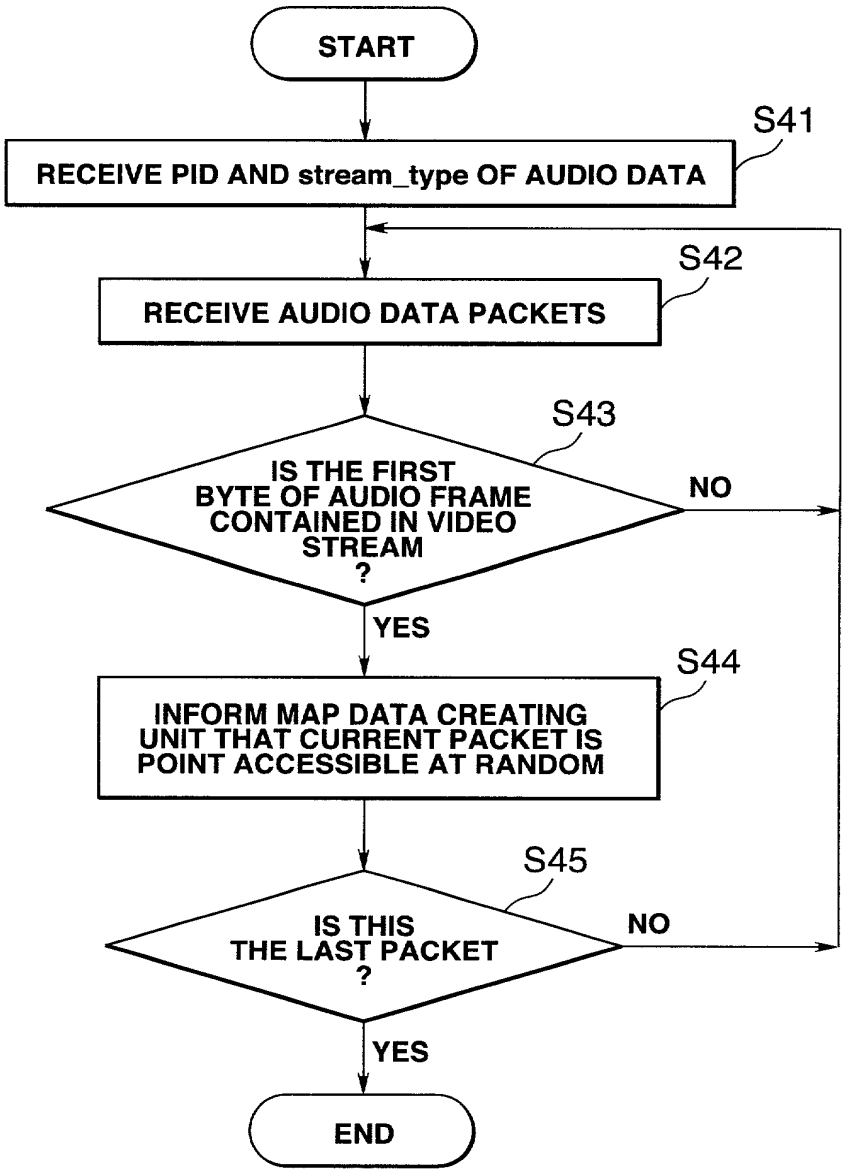

START
S41
RECEIVE PID AND stream_type OF AUDIO DATA
S42
RECEIVE AUDIO DATA PACKETS
S43
IS THE FIRST BYTE OF AUDIO FRAME CONTAINED IN VIDEO STREAM ?
NO
YES
S44
INFORM MAP DATA CREATING UNIT THAT CURRENT PACKET IS POINT ACCESSIBLE AT RANDOM
S45
IS THIS THE LAST PACKET ?
NO
YES
END

FIG.13

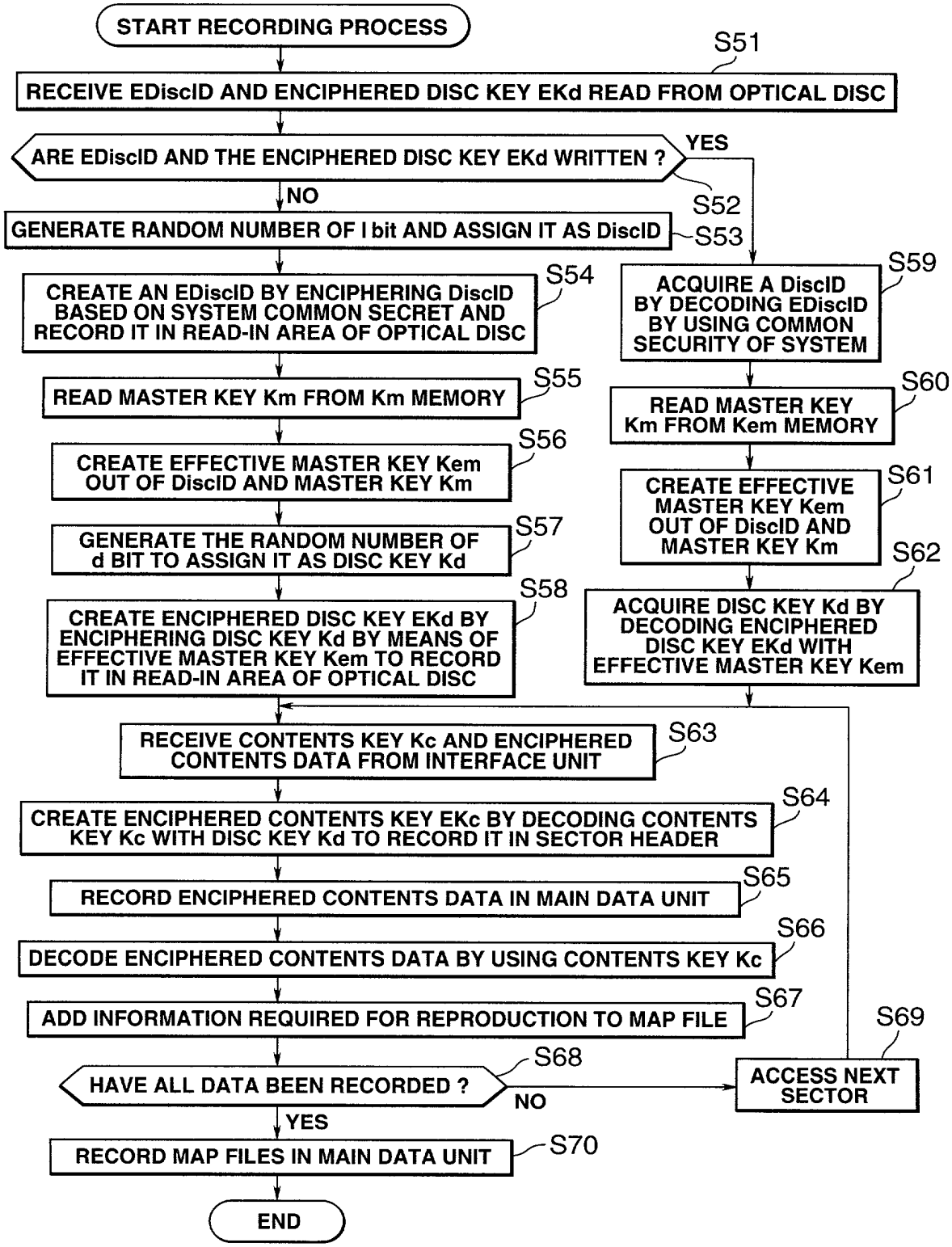

START RECORDING PROCESS
S51
RECEIVE EDiscID AND ENCIPHERED DISC KEY EKd READ FROM OPTICAL DISC
ARE EDiscID AND THE ENCIPHERED DISC KEY EKd WRITTEN ?
YES
S52
NO
GENERATE RANDOM NUMBER OF I bit AND ASSIGN IT AS DiscID
S53
CREATE AN EDiscID BY ENCIPHERING DiscID BASED ON SYSTEM COMMON SECRET AND RECORD IT IN READ-IN AREA OF OPTICAL DISC
S54
READ MASTER KEY Km FROM Km MEMORY
S55
CREATE EFFECTIVE MASTER KEY Kem OUT OF DiscID AND MASTER KEY Km
S56
GENERATE THE RANDOM NUMBER OF d BIT TO ASSIGN IT AS DISC KEY Kd
S57
CREATE ENCIPHERED DISC KEY EKd BY ENCIPHERING DISC KEY Kd BY MEANS OF EFFECTIVE MASTER KEY Kem TO RECORD IT IN READ-IN AREA OF OPTICAL DISC
S58
S59
ACQUIRE A DiscID BY DECODING EDiscID BY USING COMMON SECURITY OF SYSTEM
S60
READ MASTER KEY Km FROM Kem MEMORY
S61
CREATE EFFECTIVE MASTER KEY Kem OUT OF DiscID AND MASTER KEY Km
S62
ACQUIRE DISC KEY Kd BY DECODING ENCIPHERED DISC KEY EKd WITH EFFECTIVE MASTER KEY Kem
RECEIVE CONTENTS KEY Kc AND ENCIPHERED CONTENTS DATA FROM INTERFACE UNIT
S63
CREATE ENCIPHERED CONTENTS KEY EKc BY DECODING CONTENTS KEY Kc WITH DISC KEY Kd TO RECORD IT IN SECTOR HEADER
S64
RECORD ENCIPHERED CONTENTS DATA IN MAIN DATA UNIT
S65
DECODE ENCIPHERED CONTENTS DATA BY USING CONTENTS KEY Kc
S66
ADD INFORMATION REQUIRED FOR REPRODUCTION TO MAP FILE
S67
HAVE ALL DATA BEEN RECORDED ?
S68
NO
ACCESS NEXT SECTOR
S69
YES
RECORD MAP FILES IN MAIN DATA UNIT
S70
END

FIG.14

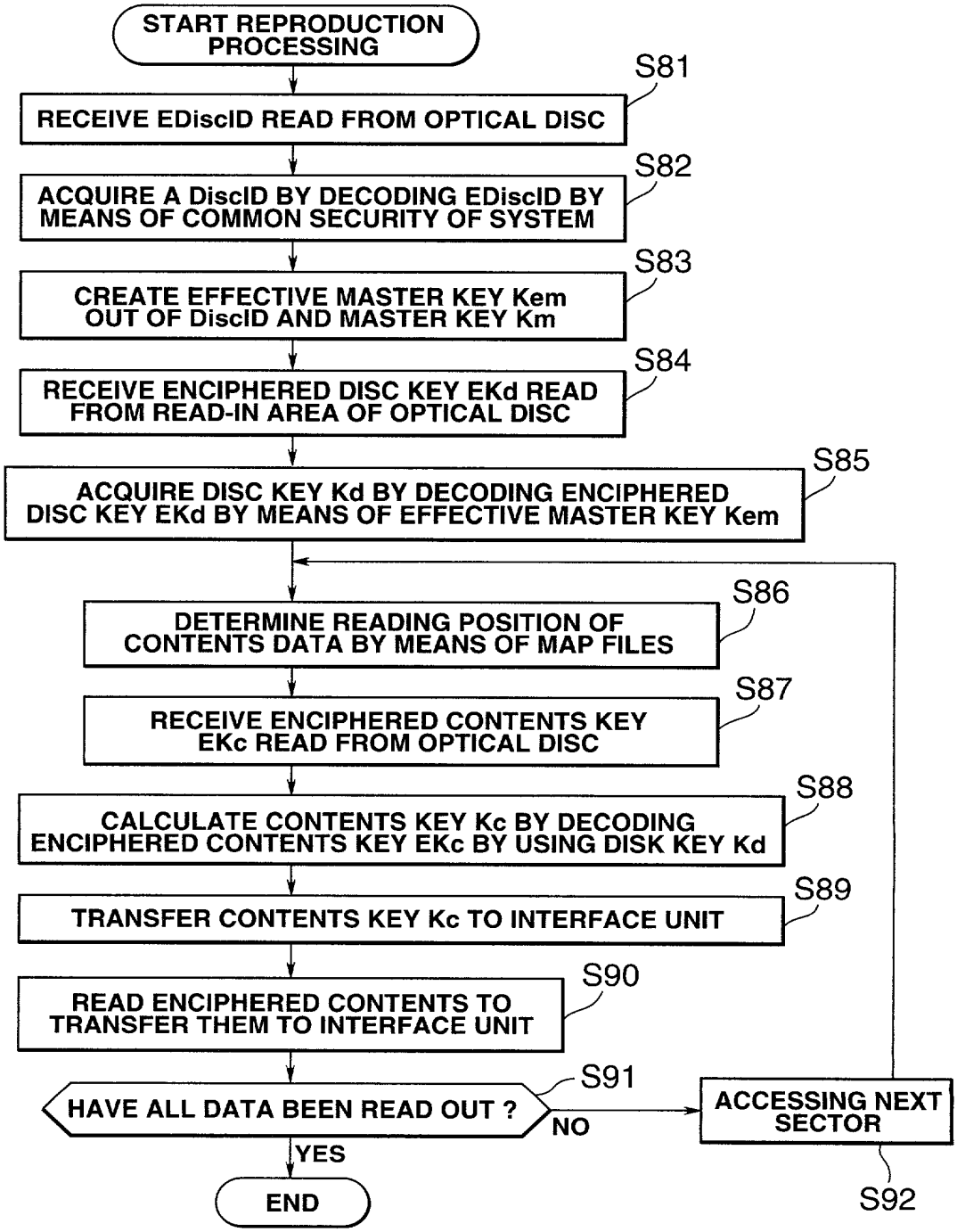

START REPRODUCTION PROCESSING
S81
RECEIVE EDiscID READ FROM OPTICAL DISC
S82
ACQUIRE A DiscID BY DECODING EDiscID BY MEANS OF COMMON SECURITY OF SYSTEM
S83
CREATE EFFECTIVE MASTER KEY Kem OUT OF DiscID AND MASTER KEY Km
S84
RECEIVE ENCIPHERED DISC KEY EKd READ FROM READ-IN AREA OF OPTICAL DISC
S85
ACQUIRE DISC KEY Kd BY DECODING ENCIPHERED DISC KEY EKd BY MEANS OF EFFECTIVE MASTER KEY Kem
S86
DETERMINE READING POSITION OF CONTENTS DATA BY MEANS OF MAP FILES
S87
RECEIVE ENCIPHERED CONTENTS KEY EKc READ FROM OPTICAL DISC
S88
CALCULATE CONTENTS KEY Kc BY DECODING ENCIPHERED CONTENTS KEY EKc BY USING DISK KEY Kd
S89
TRANSFER CONTENTS KEY Kc TO INTERFACE UNIT
S90
READ ENCIPHERED CONTENTS TO TRANSFER THEM TO INTERFACE UNIT
S91
HAVE ALL DATA BEEN READ OUT ?
NO
YES
ACCESSING NEXT SECTOR
S92
END

FIG.15

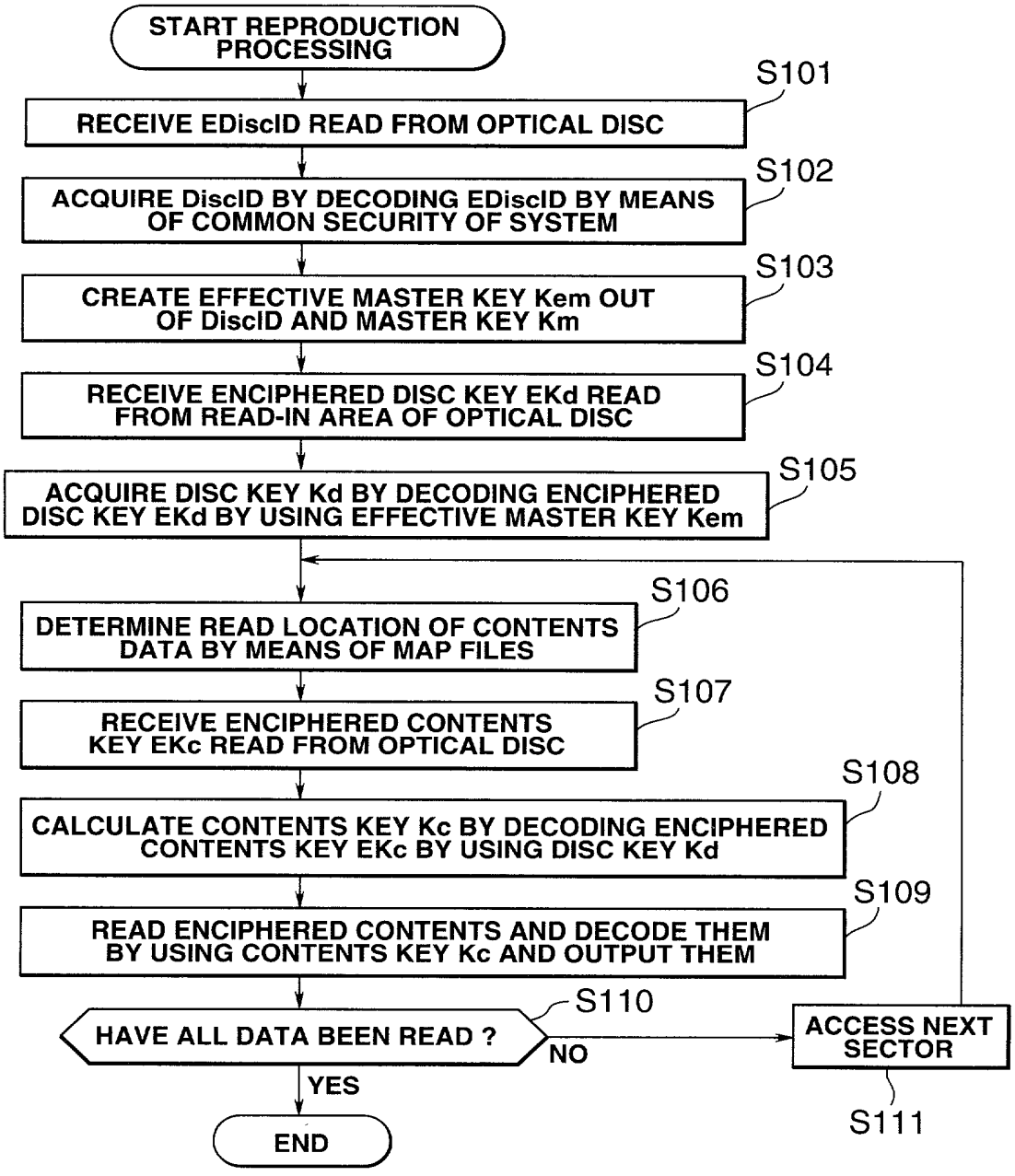

START REPRODUCTION PROCESSING
S101
RECEIVE EDiscID READ FROM OPTICAL DISC
S102
ACQUIRE DiscID BY DECODING EDiscID BY MEANS OF COMMON SECURITY OF SYSTEM
S103
CREATE EFFECTIVE MASTER KEY Kem OUT OF DiscID AND MASTER KEY Km
S104
RECEIVE ENCIPHERED DISC KEY EKd READ FROM READ-IN AREA OF OPTICAL DISC
S105
ACQUIRE DISC KEY Kd BY DECODING ENCIPHERED DISC KEY EKd BY USING EFFECTIVE MASTER KEY Kem
S106
DETERMINE READ LOCATION OF CONTENTS DATA BY MEANS OF MAP FILES
S107
RECEIVE ENCIPHERED CONTENTS KEY EKc READ FROM OPTICAL DISC
S108
CALCULATE CONTENTS KEY Kc BY DECODING ENCIPHERED CONTENTS KEY EKc BY USING DISC KEY Kd
S109
READ ENCIPHERED CONTENTS AND DECODE THEM BY USING CONTENTS KEY Kc AND OUTPUT THEM
S110
HAVE ALL DATA BEEN READ ?
NO
YES
ACCESS NEXT SECTOR
S111
END

FIG.16

S00P0914US00

PTO/SB 106 (5-00)
Approved for use through 10/31/02 OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Declaration and Power of Attorney for Patent Application

特許出願宣言書及び委任状

Japanese Language Declaration

日本語宣言書

私は、以下に記名された発明者として、ここに下記の通り宣言する：

As a below names inventor, I hereby declare that:

私の住所、郵便の宛先そして国籍は、私の氏名の後に記載された通りである。

My residence, post office address and citizenship are as stated next to my name:

下記の名称の発明について、特許請求範囲に記載され、且つ特許が求められている発明主題に関して、私は、最初、最先且つ唯一の発明者である（唯一の氏名が記載されている場合）か、或いは最初、最先且つ共同発明者である（複数の氏名が記載されている場合）と信じている。

I believe I am the original, first and sole inventor(if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled.

INFORMATION RECORDING AND/OR REPRODUCING APPARATUS

_____

_____

上記発明の明細書はここに添付されているが、下記の箱がチェックされている場合は、この限りでない：

the specification of which is attached hereto unless the following box is checked:

☐ _____ の日に出願され、
この出願の米国出願番号またはＰＣＴ国際出願番号は、
_____ であり、且つ
_____ の日に補正された出願（該当する場合）

☒ was filed on August 16, 2000
as United States Application Number of
PCT International Application Number PCT/JP00/05482
_____ and was amended on
_____ (if applicable).

私は、上記の補正書によって補正された、特許請求範囲を含む上記明細書を検討し、且つ内容を理解していることをここに表明する。

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

私は、連邦規則法典第３７編規則１．５６に定義されている、特許性について重要な情報を開示する義務があることを認める。

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

Japanese Language Declaration

日本語宣言書

私は、ここに、以下に記載した外国での特許出願または発明者証の出願、或いは米国以外の少なくとも一国を指定している米国法典第３５編第３６５条(a)によるＰＣＴ国際出願について、同第１１９条(a)-(d)項又は第３６５条(b)項に基づいて優先権を主張するとともに、優先権を主張する本出願の出願日よりも前の出願日を有する外国での特許出願または発明者証の出願、或いはＰＣＴ国際出願については、いかなる出願も、下記の枠内をチェックすることにより示した。

I hereby claim foreign priority under Title 35, United States Code, Section 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT International application which designated at least one country other than the United States listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT international application having a filing date before that of the application for which priority is claimed.

Prior Foreign Application(s)

外国での先行出願

(Number) (番号)	(Country) (国名)	(Day/Month/Year Filed)	Priority Not Claimed 優先権主張なし
11-234368	Japan	20 August 1999	☐
PCT/JP00/05482	PCT	16 August 2000	☐
			☐
			☐
			☐
			☐

私は、ここに、下記のいかなる米国仮特許出願についても、その米国法典第３５編１１９条(e)項の利益を主張する。

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any united States provisional application(s) listed below.

(Application No.) (出願番号)	(Filing Date) (出願日)

私は、ここに、下記のいかなる米国出願についても、その米国法典第３５編第１２０条に基づく利益を主張し、又米国を指定するいかなるＰＣＴ国際出願についても、その同第３６５条(c)に基づく利益を主張する。また、本出願の各特許請求の範囲の主題が、米国法典第３５編第１１２条第１段に規定された態様で、先行する米国出願又はＰＣＴ国際出願に開示されていない場合においては、その先行出願の出願日と本国内出願日またはＰＣＴ国際出願日との間の期間中に入手された情報で、連邦規則法典第３７編規則１．５６に定義された特許性に関わる重要な情報について開示義務があることを承認する。

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or 365© of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35. United States Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of application.

(Application No.) (出願番号)	(Filing Date) (出願日)	(Status: Patented, Pending, Abandoned) (現況：特許許可、係属中、放棄)

私は、ここに表明された私自身の知識に係わる陳述が真実であり、且つ情報と信ずることに基づく陳述が、真実であると信じられることを宣言し、さらに、故意に虚偽の陳述などを行った場合は、米国法典第１８編第１００１条に基づき、罰金または拘禁、若しくはその両方により処罰され、またそのような故意による虚偽の陳述は、本出願またはそれに対して発行されるいかなる特許も、その有効性に問題が生ずることを理解した上で陳述が行われたことを、ここに宣言する。

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Japanese Language Declaration

日本語宣言書

委任状： 私は本出願を審査する手続を行い、且つ米国特許商標庁との全ての業務を遂行するために、記名された発明者として、下記の弁護士及び／または弁理士を任命する。（氏名及び登録番号を記載すること）

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact al business in the Patent and Trademark Office connected therewith (list name and registration number)

WILLIAM S. FROMMER, Registration No. 25,506 and
DENNIS M. SMID, Registration No. 34,930

書類送付先

Send Correspondence to:
WILLIAM S. FROMMER, Esq.
c/o FROMMER LAWRENCE & HAUG LLP
745 Fifth Avenue
New York, New York 10151

直通電話連絡先：（氏名及び電話番号）

Direct Telephone Calls to:
(212) 588-0800
to the attention of:
WILLIAM S. FROMMER

1-00

唯一または第一発明者氏名

Full name of sole or first inventor

Tomoyuki ASANO

発明者の署名 日付

inventor's signature Date

Tomoyuki Asano March 19, 2001

住所

Residence

Kanagawa, Japan JPX

国籍

Citizenship

Japan

郵便の宛先

Post Office Address

c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan

第二共同発明者がいる場合、その氏名

Full name of second joint inventor, if any

2-00

Yoshitomo OSAWA

第二共同発明者の署名 日付

Second Inventor's signature Date

Yoshitomo Osawa 27/Mar/2001

住所

Residence

Kanagawa, Japan JPX

国籍

Citizenship

Japan

郵便の宛先

Post Office Address

c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan

（第三以下の共同発明者についても同様に記載し、署名をすること）

(Supply similar information and signature for third and subsequent joint inventors)

Japanese Language Declaration

日本語宣言書

委任状：私は本出願を審査する手続きを行い、且つ米国特許商標庁との全ての業務を遂行するために、記名された発明者として、下記の弁護士及び／または弁理士を任命する。(氏名及び登録番号を記載すること)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact al business in the Patent and Trademark Office connected therewith (list name and registration number)

書類送付先

WILLIAM S. FROMMER, Registration, No. 25,506 and
DENNIS M. SMID, Registration No. 34,930

Send Correspondence to:
WILLIAM S. FROMMER, Esq.
c/o FROMMER LAWRENCE & HAUG LLP
745 Fifth Avenue
New York, New York 10151

直通電話連絡先：(氏名及び電話番号)

Direct Telephone Calls to:
(212) 588-0800
to the attention of:
WILLIAM S. FROMMER

第三共同発明者がいる場合、その氏名

Full name of third joint inventor, if any

Motoki KATO

第三共同発明者の署名　　日付

Third inventor's signature　　Date

Motoki Kato　　March 28, 2001

住所

Residence

Kanagawa, Japan JPX

国籍

Citizenship

Japan

郵便の宛先

Post Office Address

c/o Sony Corporation, 7-35, Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo 141-0001 Japan

第四共同発明者がいる場合、その氏名

Full name of fourth joint inventor, if any

第四共同発明者の署名　　日付

Fourth Inventor's signature　　Date

住所

Residence

国籍

Citizenship

郵便の宛先

Post Office Address

sha0062